



/ GATEWAY USER MANUAL

For all Broadcom Chipset-based models including:

ADSL 3xx series

VDSL 5xx series

Release 3.4

June, 2015

Table of Contents

Table of Contents	1
Introduction	3
Disclaimer	3
FCC Interference Statement	3
FCC Caution	3
Safety Warnings	4
Welcome!	5
Purpose & Scope	5
Intended Audience	5
Getting Assistance	5
Getting Familiar With Your Gateway	6
LED Status Indicators:	6
Connections:	7
DSL	7
WAN	7
LAN	8
USB	8
POWER	8
External Buttons:	8
WPS Button	8
WLAN Button	9
Reset Button	9
Logging in to Your SmartRG Gateway's UI	9
Device Info	11
Summary	11
Wan Info	11
Statistics	12
LAN	12
WAN Service	13
xTM	14
xDSL	15
Route	19
ARP	19
DHCP	20
Advanced Setup	21
Layer2 Interface	21
ATM Interface	21
PTM Interface	23
ETH Interface	25
WAN Service	25
PPP over Ethernet	25
IP Over Ethernet	32
Ethernet Config	37
Ethernet Port Configuration	37
Model-specific variants:	37
LAN	37
Local Area Network (LAN) Setup	37
IPv6 Autoconfig	39
NAT	42
Virtual Servers (Port Forward)	42
Port Triggering	43
DMZ Host	45
Security	45
IP Filtering - Outgoing	45
IP Filtering - Incoming	46
MAC Filtering	48
Parental Control	49
Time Restriction	49
URL Filter	50

Quality Of Service	51
QoS Config	51
QoS Queue Config	53
QoS Classification	54
QoS Port Shaping	56
Routing	57
Default Gateway	57
Static Route	58
Policy Routing	58
RIP (Routing Information Protocol)	59
DNS	60
DNS Server	60
Dynamic DNS	62
Static DNS	62
DSL	63
Advanced settings for the DSL interface.	63
DSL Bonding	66
UPnP	67
DNS Proxy	68
Interface Grouping	69
IP Tunnel	70
IPv6inIPv4	70
IPv4inIPv6	71
IPSec	72
Certificate	74
Local	74
Trusted CA	76
Multicast	77
Wireless	79
Basic	79
Security	81
Manual Setup - Network Authentication: Open and Shared	83
Manual Setup - Network Authentication: 802.1X	84
Manual Setup - Network Authentication: WPA	85
Manual Setup - Network Authentication: WPA-PSK	85
Manual Setup - Network Authentication: WPA2	86
Manual Setup - Network Authentication: WPA2-PSK	87
Manual Setup - Network Authentication: Mixed WPA2-WPA	88
Manual Setup	89
Network Authentication: Mixed WPA2/WPA-PSK	89
MAC Filter	90
Wireless Bridge	91
Advanced	92
Station Info	95
Diagnostics	95
Diagnostics	96
Fault Management	96
Management Settings	97
Backup	97
Update	98
Restore Default	99
System Log	100
Security Log	101
Management Server	102
TR-069 Client	102
STUN Config	105

Internet Time	106
Access Control	107
Accounts	107
Services	110
Passwords	111
Update Software	112
Reboot	113
Appendix A: Advanced Features Overview	114
Connect- and- Surf (Automatic Broadband Connection Configuration)	114
Activation (Automatic ACS Connection Configuration)	114
TR- 069 Remote Management: Automated Configuration Server Support	114
	116
Appendix B: Feature Comparison Matrix	116
Revision History	117

Introduction

Copyright © 2014 by SmartRG, Inc.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of SmartRG, Inc.

Published by SmartRG, Inc. All rights reserved.

Disclaimer

SmartRG does not assume any liability arising out of the application or use of any products, or software described herein. Either does it convey any license under its patent rights nor patent rights of others. SmartRG further reserves the right to make changes to any products described herein without notice. This publication is subject to change without notice.

Any trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

FCC Interference Statement

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

SmartRG Inc declares that the WR100 is limited to operations on Channels 1 through 11, from 2400 to 2483.5 MHz by specified firmware controlled in the USA.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the correct supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas, or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust, or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

Welcome!

Thank you for purchasing this SmartRG product.

SmartRG proudly brings you the best, most innovative broadband gateways available. SmartRG enables service providers to monitor, manage, and monetize the connected home through the design and production of reliable and highly interoperable hardware and software solutions.

As an early innovator in TR-069 remote management technology, SmartRG offers the finest in managed broadband and home networking solutions. Our products leverage various broadband access technologies and are outfitted with highly customizable software, meeting diverse service provider requirements. Based in the USA, SmartRG provides local, proactive software development and customer support. In the rapidly evolving broadband market, SmartRG helps service providers keep their businesses on the cutting edge through its laser-focused product line, leveraging the very latest in broadband access and home networking technologies. SmartRG solutions enable service providers to improve their bottom line by reducing service costs and increasing customer satisfaction. Learn more at www.SmartRG.com.

Purpose & Scope

The purpose and scope of this document is to provide the customers of SmartRG with installation, configuration and monitoring information for all CPE platforms.

Intended Audience

The information in this document is intended for Network Architects, NOC Administrators, Field Service Technicians and other networking professionals responsible for deploying and managing broadband access networks. The reader of this manual is assumed to have a basic understanding of desktop computer operating systems, networking concepts and telecommunications.

Getting Assistance

Subscribers: If you require help with this product, please contact your service provider.

Service providers: if you require help with this product, please open a support request.

Getting Familiar With Your Gateway

This section contains a quick description of the Gateway's lights, ports, and buttons. SmartRG produces several models that vary slightly in capabilities (See Appendix B for details) but the basic scheme of lights, ports and buttons represented in this section exist on each model.

LED Status Indicators:

Your SmartRG gateway has several indicator lights (LEDs) on its front panel. The number of DSL ports or USB ports may vary from model to model but generally, these indicators are available on all models:

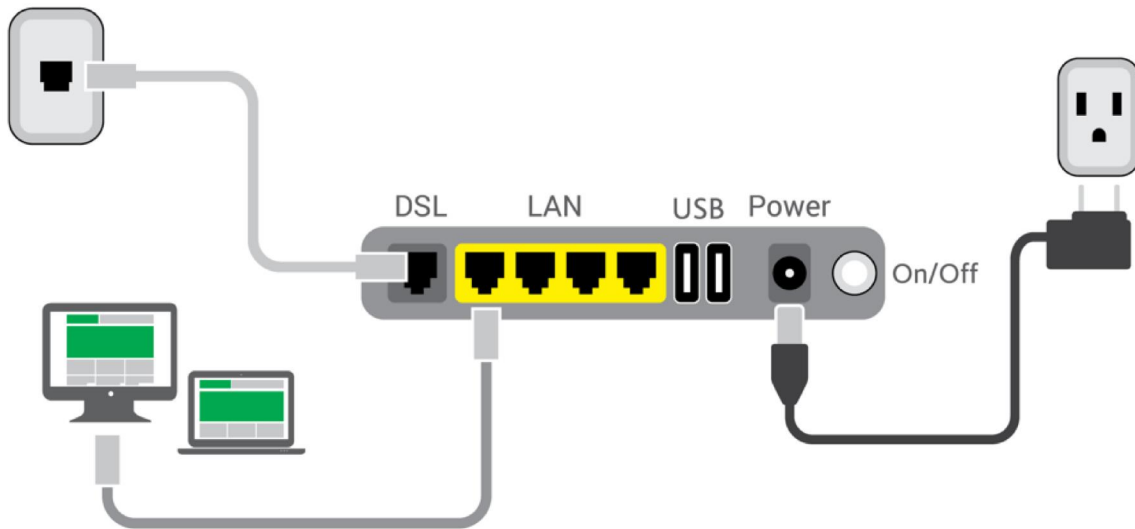
	POWER	WAN	LAN 1-4	WLAN	WPS	DSL 1 or 2	INTERNET
Power up test failure	●						
DSL sync acquired and gateway online	●					●	●
No sync to DSL line	●					○	
DSL sync in progress	●					⚙	
Modem authentication in progress	●					●	⚙
DSL sync acquired and gateway online	●					●	●
Gateway online and data transfer in progress	●					●	⚙
IP connection failure	●						○
Connection dropped – attempting re-authentication	●	○				○	●
LAN device on network connected	●		●				
Wi-Fi enabled on modem	●			●			
PC / network activity / data transfer	●	●/⚙	●/⚙	●/⚙			●/⚙
WPS Setup procedure in progress	●			●	⚙		
Failure to find any partner with which to pair	●				●		
Session overlap detected. Possible security risk	●				⚙		
WPS Connection completed successfully	●			●	●		

● : On ○ : Off ⚙ : Blinking / active

Connections:

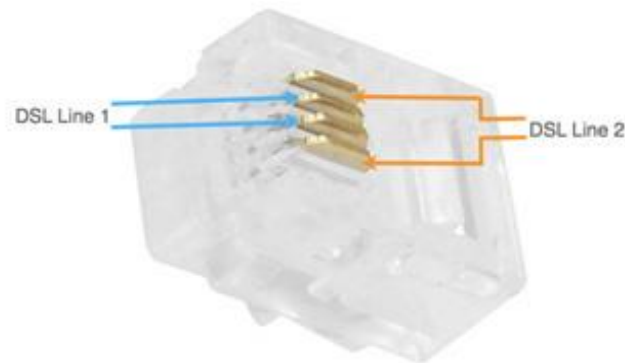
Below is a generic representation of a SmartRG gateway, however your specific model may have greater or fewer ports and controls across the back of the unit. Refer to the Quick Start Guide enclosed with your gateway for specifics regarding installation of your particular model.

The ports depicted in this example are described as follows:



DSL

The grey, RJ12 port labeled DSL is specifically intended for connection to an internet provider via a DSL (Digital Subscriber Line) service. The center pair carries the first DSL line. For models like the SR550n equipped with two DLS ports and bonded DSL capability, the outer pair carries the second line.



WAN

A stand-alone RJ45 port labeled WAN enables your SmartRG gateway to be hard-wired to another network device with a RJ45/Ethernet output such as a cable, fiber, or DSL modem.

For models with a stand-alone, RJ45, WAN port and a DSL port, the WAN port can be re-purposed to function as an additional LAN port when your internet connection is via DSL.

See the [ETH Interface](#) section of this manual for further instructions to enable this SmartPort™ feature.

LAN

The set of four, RJ45 ports across the back of your gateway labeled LAN1, LAN2, LAN3, LAN4 are the means to connect client devices such as computers and printers to your gateway.

On some models, one of these four ports may be labeled as WAN indicating SmartPort™ support. SmartPort™ enables a LAN port to be re-purposed to function as an Ethernet WAN port (describe above). When this port is serving as a LAN port, the corresponding LED on the face of the unit is labeled, "WAN".

See the [ETH Interface](#) section of this manual for further instructions to enable this SmartPort™ feature.

USB

USB ports on SmartRG products currently provide +5 DC volts. Future firmware updates will enable data transfer via USB.

POWER

Use only the power supply included with your gateway. Intended for indoor use only.

External Buttons:

Smart RG gateways provide pushbutton controls on the exterior for critical features. These buttons give you a convenient means to, trigger WPS mode, toggle the WiFi radio on and off or reset the gateway.

The following describes specifics for each of these controls.

WPS Button

Wi-Fi Protected Setup™ (WPS) is standard means for secure connection between your gateway and various wireless client devices. It is designed to simplify the pairing process between devices.

If you have client devices that support WPS, use this to automatically configure wireless security for your network. WPS configures one client device at a time. Reference the Quick Start Guide included with your gateway for specific instructions. Also see the [Wireless](#) chapter of this manual.

Repeat the steps as necessary for each additional WPS compliant device you wish to connect.

The location of the WPS button varies by model.

- On models SR550n, SR510n, and SR552n, the button is located on the left side of the unit.
- SR360n, locate the WPS button on the top of the unit.
- For the SR350n and SR500n models, an exterior button is not present however WPS is supported via the on-board software.

Reference the Quick Start Guide included with your gateway for specific instructions.

WLAN Button

The button labeled WiFi or WLAN (depending on model) toggles the WiFi radio on and off. Refer to the WLAN LED indicator to determine the current state of the WiFi radio.

The location of the WLAN button varies by model.

- On models SR360n, SR550n, SR510n, SR552n the button is located on the left side of the unit.
- For the SR350n and SR500n models, an exterior button is not present however WPS is supported via the on-board software. Reference the Quick Start Guide included with your gateway for specific instructions.

To ACTIVATE

Press and hold the WiFi (WLAN) button for 3-5 seconds then release. Expect a 1-3 second delay before the WIFI (WLAN) LED turns on. The WiFi radio is now on.

To DEACTIVATE:

Press and hold the WiFi (WLAN) button for 3-5 seconds then release. Expect a 1-3 second delay before the WIFI (WLAN) LED turns off. The WiFi radio is now off.

Reset Button

The Reset button is a small hole in the gateway's enclosure with the actual button mounted behind the surface. This style of pushbutton prevents the gateway from being inadvertently reset during handling. Reset must be actuated with a paper clip or similar implement. This pin-hole sized reset button has three functions. The duration for which the button is held dictates which function is carried out.

DURATION TO HOLD RESET BUTTON	EFFECT
Less than 6 seconds	Performs a modem reset that is equivalent to the Reboot function in the gateway's software UI.
6-20 seconds	Performs the software UI equivalent to Restore Default function.
20 or more seconds	The POWER LED goes red and unit enters CFE mode. A state associated with performing firmware updates via Internet browser.

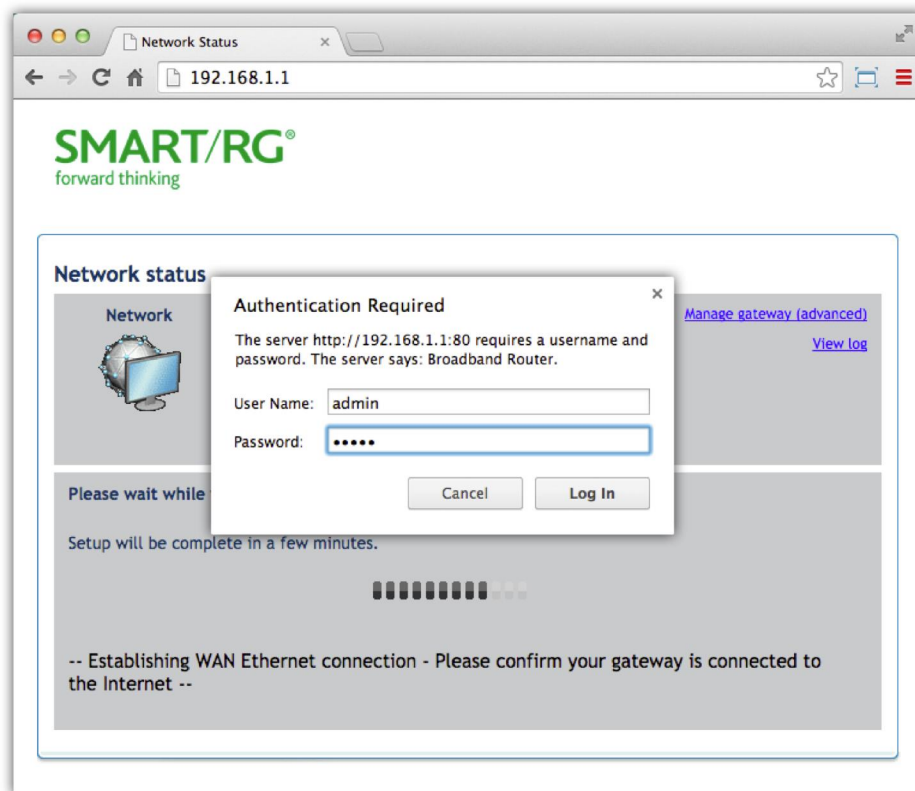
The location of the Reset button varies by model.

- On models SR500n, SR505n, SR510n, SR550n, SR552n and SR630n, the button is located on the rear of the unit.
- For the SR350n, locate the Reset button on the bottom of the unit.
- For the SR360n, locate the Reset button on the left side of the unit.

Logging in to Your SmartRG Gateway's UI

To manually configure the SmartRG [Gateway](#), access the gateway's embedded web UI:

1. Attach your computer's RJ45 connection to any of the SmartRG gateway's LAN ports (1-4).
2. Configure your computer's IP interface to acquire an IP address using DHCP. (See the IMPORTANT note below for instructions on logging in to a SmartRG gateway configured for "bridge mode" operation.)
3. Open a browser and enter the gateway's default address <http://192.168.1.1> in the address bar.
4. Click the [Manage Gateway \(Advanced\)](#) link in the upper right.
5. Enter the default username and password: admin/admin and click [Login](#) to display the [Device Info](#) page.



NOTE: The gateway's UI can be accessed via the WAN connection by entering the WAN IP address in your browser's address bar and entering the default username and password: support/support. WAN HTTP [access control](#) MUST be enabled to access the gateway's UI via the WAN connection. Reference section on [Management Access Control](#) for details.

If your SmartRG gateway is configured for "bridge mode" (modem) operation, your PC will NOT be able to acquire an address via CPE's DHCP. Instead, manually configure your PC's interface with an IP address on the default network (e.g. 192.168.1.100).

The balance of this guide is dedicated to a sequential walk-through of the user interface of your gateway. Here you will find a visual reference of each screen along with a Description for each of the parameters displayed. Where applicable, a range of valid values is outlined along with an overview narrative of each screen.

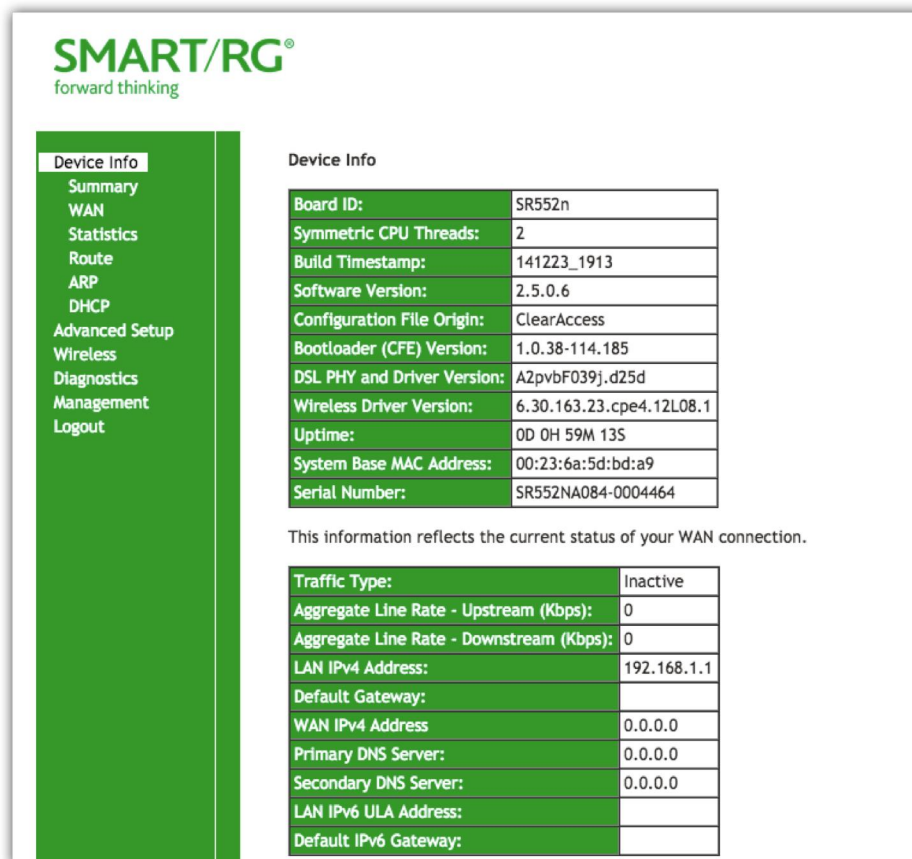
For in depth "how-to" information for specific scenarios, please take advantage of the knowledge base found at our support web site. Access to this site is restricted to SmartRG customers and partners. Do not attempt to share links to this site with your subscribers.

Device Info

There are nine selections under Device Info in the left navigation bar. Each of them shows a different element of the gateway's setup, status or nature of its connection with the provider and also with LAN devices. Device Info screens are read-only. It is not possible to interact with or change the settings in this section.

Summary

Upon successful login, **Device Info** is the first screen to appear. This screen is dedicated to the display of hardware and software details associated with your gateway. In addition, the current status of the WAN connection (if present) is shown.



SMART/RG®
forward thinking

Device Info

Board ID:	SR552n
Symmetric CPU Threads:	2
Build Timestamp:	141223_1913
Software Version:	2.5.0.6
Configuration File Origin:	ClearAccess
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	AZpvbF039j.d25d
Wireless Driver Version:	6.30.163.23.cpe4.12L08.1
Uptime:	0D 0H 59M 13S
System Base MAC Address:	00:23:6a:5d:bd:a9
Serial Number:	SR552NA084-0004464

This information reflects the current status of your WAN connection.

Traffic Type:	Inactive
Aggregate Line Rate - Upstream (Kbps):	0
Aggregate Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
WAN IPv4 Address:	0.0.0.0
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	

Wan Info

The Device Info WAN status screen, provides a high level overview for the connection between your Internet Service Provider and the Gateway device, itself. The WAN interface could physically be DSL or Ethernet and supports a number of Layer 2 and above configuration options covered later in this document. Some features are supported only on specific SmartRG models. These exceptions and are specified in this guide.



Device Info
Summary
WAN
Statistics
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management
Logout

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ptm0	ipoe_0_0_1	IPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Unconfigured	0.0.0.0	(null)

The individual fields on this screen are defined as follows:

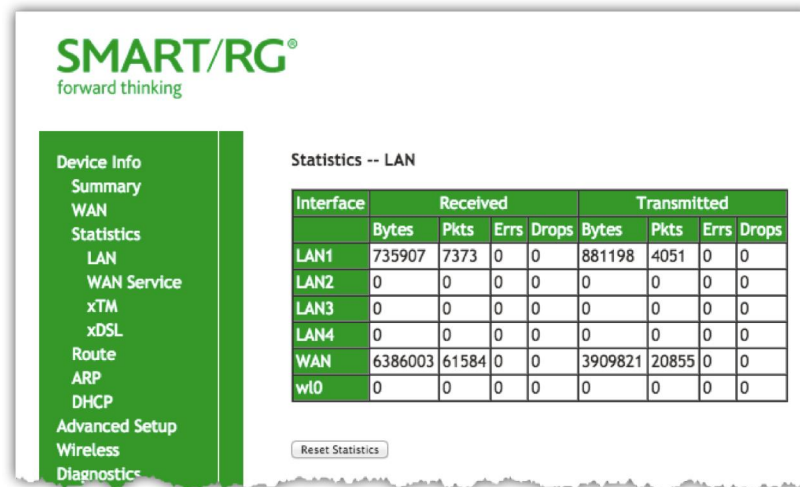
Field Name	Description
Interface	Displays the connection interface (layer 2 interface () through which gateway handles the traffic.)
Description	Displays the service description (pppoe, ipoe, br)
Type	Displays the service type (PPPoE, IPoE, Bridge)
VlanMuxId	Displays the VLAN ID (Disabled, 0-4094)
IPv6	Displays the state of IPv6 (Enabled, Disabled)
Igmp	Displays the state of IGMP (Enabled, Disabled)
MLD	Displays the state of MLD (Enabled, Disabled)
NAT	Displays the state of NAT (Enabled, Disabled)
Firewall	Displays the state of the Firewall (Enabled, Disabled)
Status	Displays the status of the WAN connection (Disconnected, Unconfigured, Connecting, Connected)
IPv4 Address	Displays the obtained IPv4 address
IPv6 Address	Displays the obtained IPv6 address

Statistics

The Statistic screens provide network interface information for LAN, WAN Service, xTM and DSL. All data is updated on a 15 minute interval.

LAN

Device Info -> Statistics -> LAN displays the TX/RX Bytes, Packets, Error and Drops for each LAN interface for your SmartRG modem. All local LAN Ethernet ports, Ethernet WAN ports and w10 (Wireless Interface) for your SmartRG gateway are included.



Use the [Reset Statistics](#) button near the bottom of the screen to reset these counters.

NOTE: Not all SmartRG gateway models support the SmartPort feature wherein a LAN port can be re-purposed to function as a WAN port (as displayed in the [Interface](#) column below note, LAN3, LAN2, LAN1, WAN.) Only models SR5xxn and SR360n support this functionality.

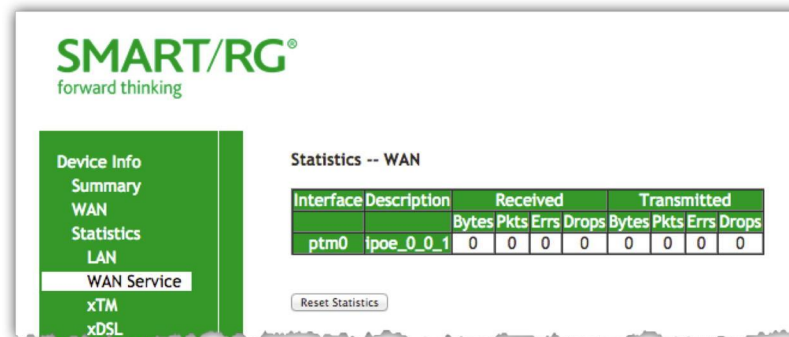
The individual fields on this screen are defined as follows:

Field Name	Description
Interface (Received/ Transmitted)	LAN1, LAN2, LAN3, LAN4 Ethernet WAN if configured on your device wl0 is the Wireless LAN side Interface
Interface	Displays available LAN interfaces
Bytes	Bytes - (RX/ TX) total quantity of packets in Bytes
Pkts	Pkts - (RX/ TX) total quantity of packets
Errs	Errs - (RX/ TX) total quantity of error packets
Drops	Drops - (RX/ TX) total quantity of dropped packets

WAN Service

[Device Info](#) -> [Statistics](#) -> [WAN](#) displays the TX/RX Bytes, Packets, Error and Drops for each WAN interface for your SmartRG Gateway. All WAN interfaces configured for your SmartRG gateway are included.

Use the [Reset Statistics](#) button near the bottom of the screen to reset these counters.



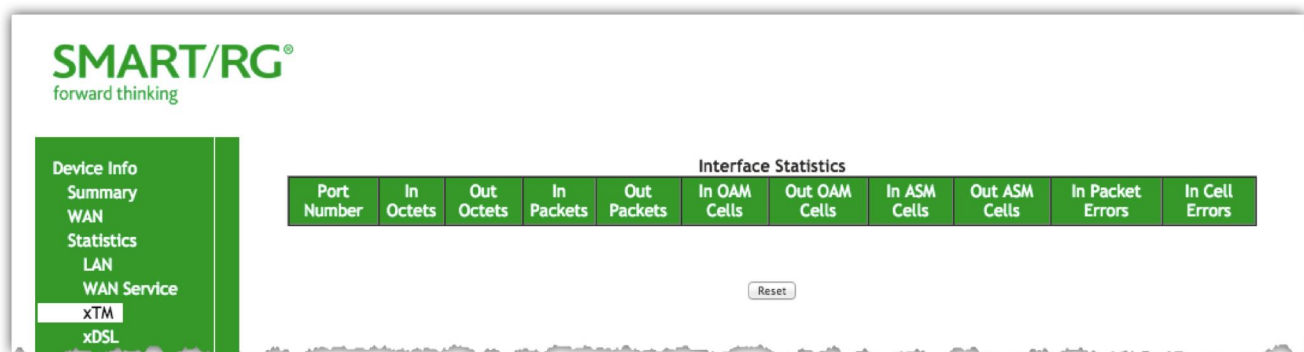
The individual fields on this screen are defined as follows:

Field Name	Description
Interface (RX/ TX)	Displays available WAN interfaces (atm, ptm, eth)
Description (RX/ TX)	Displays the service description (pppoe, ipoe, b)
	Bytes - (RX/ TX) total quantity of packets in Bytes
	Pkts - (RX/ TX) total quantity of packets
	Errs - (RX/ TX) total quantity of error packets
	Drops -(RX/ TX) total quantity of dropped packets
Reset Statistics	Resets the Statistics to zero.

xTM

The [Device Info -> Statistics -> xTM](#) displays the ATM/PTM statistics for your SmartRG Gateway. All WAN interfaces configured for your SmartRG gateway are included.

Use the [Reset](#) button near the bottom of the screen to reset these counters.



The individual fields on this screen are defined as follows:

Field Name	Description
Port Number	Displays the statistics specifically for Port 1, or both ports if Bonded
In Octets	Total quantity of received Octets
Out Octets	Total quantity of transmitted Octets
In Packets	Total quantity of received Packets
Out Packets	Total quantity of transmitted Packets
In OAM Cells	Total quantity of received OAM Cells
Out OAM Cells	Total quantity of transmitted OAM Cells
In ASM Cells	Total quantity of received ASM Cells
Out ASM Cells	Total quantity of transmitted ASM Cells
In Packet Errors	Total quantity of received Packet Errors
In Cell Errors	Total quantity of received Cell Errors

xDSL

Device Info -> Statistics -> xDSL displays the DSL statistics for your SmartRG Gateway. All xDSL (VDSL or ADSL) interfaces configured for your SmartRG gateway are included. You are also able to reset these counters by selecting the Reset Statistics button located on the xTM screen as shown below. This section explains each of these statistics. The terms and their explanations are derived from the relevant ITU--T standards and referenced accordingly.

Use the **Reset Statistics button** near the bottom of the screen to reset these counters.

Also featured is an xDSL Bit Error Rate (BER) test which determines the quality of the xDSL connection. Scroll to the bottom of the table of statistics and click xDSL BER Test. The test transfers idle cells containing a known pattern and compares the received data with this known pattern. Comparison errors are then tabulated and displayed. The duration of the test is selectable from the drop-down menu at the test screen. Selectable values range from 1-360 seconds.

The following figure and table depict and explain the fields on the screen..

SMART/RG®

forward thinking

Device Info
Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management
Logout

Statistics -- xDSL

Bonding Line Selection line 1

Mode:		
Traffic Type:		
Status:		
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test
Reset Statistics

The individual fields on this screen are defined as follows:

Field Name	Description
Mode	Displays the xDSL mode that the modem has trained under (e.g. ADSL2+, G.DMT, etc).
Traffic Type	Displays the connection type (ATM, PTM, ETH)
Status	Displays the status of the connection (Up, NoSignal, Initializing)
Link Power State	The current link power management state (e.g. L0, L2, L3).
Line Coding (Trellis)	(Downstream/Upstream) Displays the state of Trellis Coded Modulation (On, Off)
SNR Margin (db)	(Downstream/Upstream) The signal-to-noise ration margin (SNRM) is the maximum increase (in dB) of the received noise power, such that the modem can still meet all of the target BERs over all the frame bearers. [2]

Field Name	Description
Attenuation (db)	(Downstream/Upstream) The signal attenuation is defined as the difference in dB between the power received at the near-end and that transmitted from the far-end. [2]
Output Power (dBm)	(Downstream/Upstream) Transmit power from the gateway to the DSL loop relative to one Milliwatt (dBm).
Attainable Rate (Kbps)	(Downstream/ Upstream) The typically obtainable sync rate. The attainable net data rate that the receive PMS-TC and PMD functions are designed to support under the following conditions: • Single frame bearer and single latency operation • Signal-to-Noise Ratio Margin (SNRM) to be equal or above the SNR Target Margin • BER not to exceed the highest BER configured for one (or more) latency paths • Latency not to exceed the highest latency configured for one (or more) latency paths • Accounting for all coding gains available (e.g. trellis coding, RS FEC) with latency bound • Accounting for the loop characteristics at the instant of measurement [2]
PhyR Status	[Inactive, Active] Physical Layer Retransmission feature status. (Downstream/ Upstream)
Rate (Kbps)	(Path 0/1, Downstream/Upstream) The current net data rate of the xDSL link. Net data rate is defined as the sum of all frame bearer data rates over all latency paths. [2]
MSGc (# of bytes in overhead channel message)	(Path 0/1, Downstream/Upstream) The number of bytes in the message-based portion of the overhead structure.
B (# of bytes in Mux Data Frame)	(Path 0/1, Downstream/Upstream) The nominal number of bytes from frame bearer #n per Mux Data Frame at Reference Point A in the current latency path.
M (# of Mux Data Frames in FEC Data Frame)	(Path 0/1, Downstream/Upstream) The number of Mux Data Frames per FEC Data Frame in the current latency path.
T (Mux Data Frames over sync bytes)	(Path 0/1, Downstream/Upstream) The ratio of the number of Mux Data Frames to the number of sync bytes in the current latency path.
R (# of check bytes in FEC Data Frame)	(Path 0/1, Downstream/Upstream) The number of Reed Solomon redundancy bytes per codeword in the current latency path. This is also the number of redundancy bytes per FEC Data Frame in the current latency path.
S (ratio of FEC over PMD Data Frame length)	(Path 0/1, Downstream/Upstream) Ratio of FEC over PMD Data Frame length.
L (# of bits in PMD Data Frame)	(Path 0/1, Downstream/Upstream) The number of bits from the latency path included per PMD.Bits.confirm primitive (PMD Data Frame).
D (interleaver depth)	(Path 0/1, Downstream/Upstream) The interleaving depth in the current latency path.
Delay (msec)	(Path 0/1, Downstream/Upstream) The PMS-TC delay in milliseconds of the current latency path (or the lowest latency path when running dual-latency paths).
INP (DMT symbol)	(Path 0/1, Downstream/Upstream)
Super Frames	(Path 0/1, Downstream/Upstream) The number of xDSL Super Frames transmitted/received.
Super Frame Errors	(Path 0/1, Downstream/Upstream) The number of xDSL Super Frames transmitted/received with errors.
RS Words	(Path 0/1, Downstream/Upstream) The number of Reed-Solomon-based Forward Error Correction (FEC) codewords transmitted/received.
RS Correctable Errors	(Path 0/1, Downstream/Upstream) The number of Reed-Solomon-based FEC codewords received with errors that have been corrected.
RS Uncorrectable Errors	(Path 0/1, Downstream/Upstream) The number of Reed-Solomon-based FEC codewords received with errors that were not correctable.
RS Codewords Received	(Path 0/1, Downstream/Upstream) Total number of Reed-Solomon Codewords received.
RS Codewords Corrected	(Path 0/1, Downstream/Upstream) Total number of Reed-Solomon Codewords corrected.

Field Name	Description
RS Codewords Uncorrected	(Path 0/1, Downstream/Upstream) Total number of Reed-Solomon Codewords Uncorrected
HEC Errors	(Path 0/1, Downstream/Upstream) A count of ATM HEC errors detected. As per ITU-T G.992.1 and G.992.3, a1-byte HEC is generated for each ATM cell header. Error detection is implemented as defined in ITU-T I.432.1 with the exception that any HEC error shall be considered as a multiple bit error, and therefore, HEC Error Correction is not performed. [1],[2]
OCD Errors	(Path 0/1, Downstream/Upstream) Total number of Out-of-Cell Delineation errors. ATM Cell delineation is the process which allows identification of the cell boundaries. The HEC field is used to achieve cell delineation. [4] An OCD Error is counted when the cell delineation process transitions from the SYNC state to the HUNT state. [2]
LCD Errors	(Path 0/1, Downstream/Upstream) Total number of Loss of Cell Delineation errors. An LCD Error is counted when at least one OCD error is present in each of four consecutive overhead channel periods and SEF (Severely Errored Frame) defect is present. [2]
Total Cells	(Path 0/1, Downstream/Upstream) The total number of cells (OAM and Data cells) transmitted/received.
Data Cells	(Path 0/1, Downstream/Upstream) The total number of data cells transmitted/received.
Bit Errors	(Path 0/1, Downstream/Upstream) The total number of Idle Cell Bit Errors in the ATM Data Path. [3]
Total ES	(Downstream/Upstream) Total number of Errored Seconds. This parameter is a count of 1-second intervals with one or more CRC-8 anomalies. [4]
Total SES	(Downstream/ Upstream) Total number of Severely Errored Seconds. An SES is declared if, during a 1-second interval, there are 18 or more CRC-8 anomalies in one or more of the received bearer channels, or one or more LOS (Loss of Signal) defects, or one or more SEF (Severely Errored Frame) defects, or one or more LPR (Loss of Power) defects. [4]
Total UAS	(Downstream/Upstream) Total number of Unavailable Seconds. This parameter is a count of 1-second intervals for which the xDSL line is unavailable. The xDSL line becomes unavailable at the onset of 10 contiguous SES's. These 10 SES's shall be included in the unavailable time. Once unavailable, the xDSL line becomes available at the onset of 10 contiguous seconds with no SES's. These 10 seconds with no SES's shall be excluded from unavailable time. [4]

REFERENCES:

[1] ITU-T Recommendation G.992.1 (1999), Asymmetric digital subscriber line (ADSL) transceivers.
<http://www.itu.int/rec/T-REC-G.992.1/en>

[2] ITU-T Recommendation G.992.3 (2005), Asymmetric digital subscriber line transceivers 2 (ADSL2).
<http://www.itu.int/rec/T-REC-G.992.3/en>

[3] ITU-T Recommendation G.997.1 (2006), Physical layer management for digital subscriber line (DSL) transceivers.
<http://www.itu.int/rec/T-REC-G.997.1/en>

[4] ITU-T Recommendation I.432.1 (1999), B-ISDN user-network interface – Physical layer specification: General characteristics.
<http://www.itu.int/rec/T-REC-I.432.1/en>

Route

The [Device Info -> Route](#) displays the LAN and WAN route table information configured in your SmartRG Gateway for both IPv4 and IPv6 implementation.

SMART/RG®
forward thinking

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

IPv6 Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

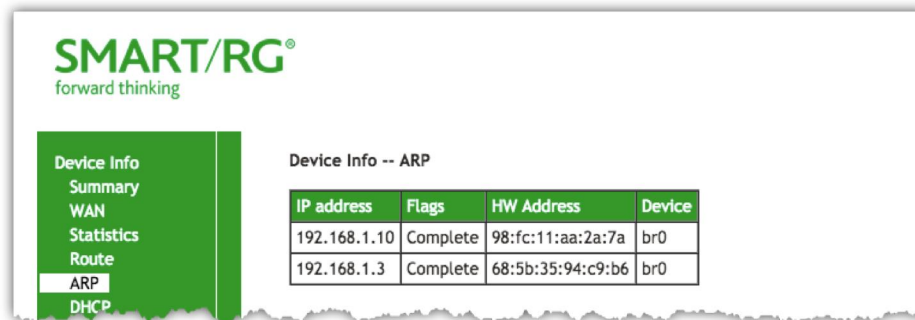
Destination	Next Hop	Flag	Metric	Service	Interface
/64	::	U	256		br0
fe80::/64	::	U	256		eth4
fe80::/64	::	U	256		eth3

The individual fields on this screen are defined as follows:

Field Name	Description
Destination (Including IPv6 Route)	Displays the Destination IP addresses.
Gateway	Displays the Gateway IP address.
Subnet Mask	Displays the Subnet Masks.
Flag (Including IPv6 Route)	Displays the status of the flags.
Metric (Including IPv6 Route)	Displays the number of hops to reach the default gateway.
Service (Including IPv6 Route)	Displays the service type.
Interface (Including IPv6 Route)	Displays the WAN/LAN interface.
Next Hop (IPv6 Route only)	Displays the next hop IP address.

ARP

[Device Info -> ARP](#) displays the host IP addresses and their hardware (MAC) addresses for each LAN Client connected to the SmartRG Gateway via a LAN Ethernet port or Wireless LAN.

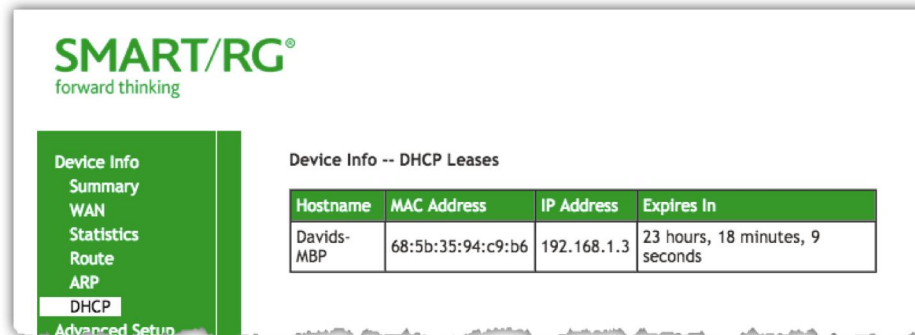


The individual fields on this screen are defined as follows:

Field Name	Description
IP address	The IP address of the host.
Flags	[Complete, Permanent, Published] Each entry in the ARP cache will be marked with one of these flags.
HW Address	The hardware (MAC) address of the host.
Device	[br(n), atm(n), eth(n), atm(n)] The system level interface by which the host is connected.

DHCP

Device Info -> DHCP displays a list of locally connected LAN hosts and their DHCP lease status, which are directly connected to the SmartRG Gateway via a LAN Ethernet port or Wireless LAN.



The individual fields on this screen are defined as follows:

Field Name	Description
Hostname	Displays the Host name of each connected LAN device.
MAC Address	Displays the MAC Address for each connected LAN device.
IP Address	Displays the IP Address for each connected LAN device.
Expires In	Displays the time until the DHCP lease expires for each LAN device.

Advanced Setup

Layer2 Interface

ATM Interface

From this screen you can configure Asynchronous Transfer Mode / Permanent Virtual Conduit for your gateway. You can customize latency options, Link Type, Encapsulation mode and more. Note that devices (routers) on both ends of the connection must support ATM / PVC.

ATM is becoming popular as a wide-area network (WAN) medium. ATM offers small cell size and strict quality of service, allowing voice, video, and data to coexist.

Terms:

- VPI - Virtual Path Identifier
- VCI - Virtual Circuit Identifier
- VC - Virtual Circuit

After selecting [Advanced Setup](#) -> [Layer2 Interface](#) -> [ATM Interface](#) from the left navigation bar, click [Add](#) in the center pane. The following screen will appear. When your desired settings have been declared, click the [Apply/Save](#) button to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]
VCI: [32-65535]

Select DSL Latency
☒ Path0 (Fast)
☐ Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
☒ EoA
☐ PPPoA
☐ IPoA

Encapsulation Mode:

Service Category:

Minimum Cell Rate: [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue
☒ Weighted Round Robin
☐ Weighted Fair Queuing

Default Queue Weight: [1-63]
Default Queue Precedence: [1-8] (lower value, higher priority)

VC WRR Weight: [1-63]
VC Precedence: [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

The individual fields on this screen are defined as follows:

Field Name	Description
VPI	[0-255] Enter a Virtual Path Identifier. VPI is an 8bit identifier to uniquely identify a network path for ATM cell packets to reach its destination. Every ATM path requires a unique VPI number to associate. Works together with the VCI. Each individual DSL circuit cannot have the same VPI/VCI combination.
VCI	[32-65535] Enter a Virtual Channel Identifier. VCI is a 16bit identifier that has a unique channel.
Select Latency	DSL: [Path0 Fast] No error correction and can provide lower latency on error free lines. [Path1 Interleaved] Error checking that provides error free data which increases latency. [Path0&1 Both] Fast & Interleaved
Link Type	[EoA] Ethernet over ATM [PPPoA] Point-to-Point Protocol over ATM [IPoA] Internet Protocol over ATM

Field Name	Description
Encapsulation Mode	[LLC/SNAP-BRIDGING] Logical Link Control used to carry multiple protocols in a single PVC (Permanent Virtual Circuit). [VC/MUX] Virtual Circuit Multiplexer creates a virtual connection used to carry one protocol per PVC (Permanent Virtual Circuit).
Service Category	[UBR without PCR] Unspecified Bit Rate with no Peak Cell Rate, flow control or time synchronization between the traffic source and destination. Commonly used with applications that can tolerate data / packet loss. [UBR with PCR] Same as above but with a Peak Cell Rate. [CBR] Constant Bit Rate relies on timing synchronization to make the network traffic predictable. Used commonly in Video and Audio traffic network applications. [NON Realtime VBR] Non Realtime Variable Bit Rate used for connections that transport traffic at a Variable Rate but need to have a guaranteed bandwidth and latency. This category does not rely on timing synchronization between the destination and source. [Realtime VBR] Realtime Variable Bit Rate. Same as above but relies on timing and synchronization between the destination and source. Commonly used in networks with compressed video traffic.
Minimum Cell Rate	[cells/s] (-1 indicates no shaping) Minimum allowable rate at which cells can be sent on a ATM network.
Scheduler for Queues of Equal Precedence as the Default Queue	The algorithm used to schedule the queue behavior. [WRR] Weighted Round Robin packets are accessed in a round robin style and classes can be given. [WFQ] Weighted Fair Queuing packets are assigned in a specific queue. Default Queue Weight [1-63] The default weight of the specified queue. Default Queue Precedence [1-8] The Precedence of the specified group. VC scheduling is unique from Default Queues.

PTM Interface

The SmartRG gateway's VDSL2 standards support Packet Transfer Mode (PTM). An alternative to ATM mode, PTM transports packets (IP, PPP, Ethernet, MPLS, and others) over DSL links. Reference the IEEE802.3ah standard for Ethernet in the First Mile (EFM) for additional information.

After selecting [Advanced Setup](#) -> [Layer2 Interface](#) -> [PTM Interface](#) from the left navigation bar, click Add in the center pane. The following screen will appear.

When your desired settings have been entered, click the [Apply/Save](#) button to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding

PTM Configuration

This screen allows you to configure a PTM flow.

Select DSL Latency
☒ Path0 (Fast)
☐ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue
☒ Weighted Round Robin
☐ Weighted Fair Queuing

Default Queue Weight: [1-63]
 Default Queue Precedence: [1-8] (lower value, higher priority)

Default Queue Minimum Rate: [1-0 Kbps] (-1 indicates no shaping)
 Default Queue Shaping Rate: [1-0 Kbps] (-1 indicates no shaping)
 Default Queue Shaping Burst Size: [bytes] (shall be >=1600)

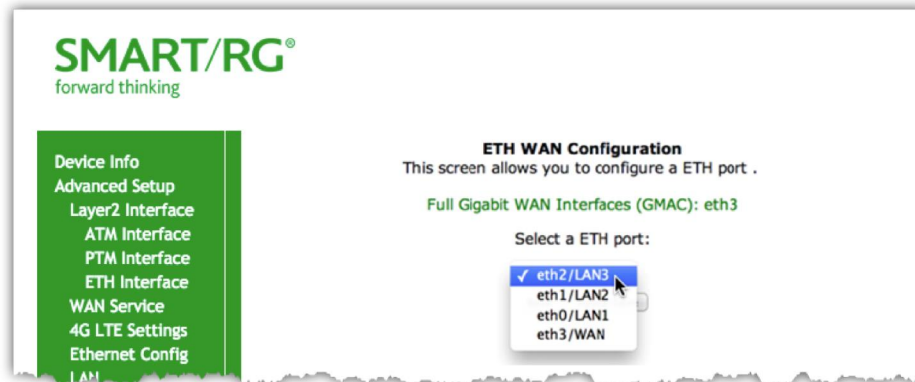
[Back](#) [Apply/Save](#)

The individual fields on this screen are defined as follows:

Field Name	Description
Select DSL Latency	[Path0 Fast] No error correction and can provide lower latency on error free lines. [Path1 Interleaved] Error checking that provides error free data. This tends to increase latency. [Path0&1 Both] Fast & Interleaved.
Weighted Round Robin	Time slices are assigned to each process in equal portions and in circular order, handling all processes without priority (also known as cyclic executive).
Weighted Fair Queuing	A data packet scheduling technique allowing different scheduling priorities to statistically multiplex data flows. Since each data flow has its own queue, an ill-behaved flow (who has sent larger packets or more packets per second than the others since it became active) will only punish itself and not other sessions.
Default Queue Weight	[1-63] Enter a default weight of the specified queue.
Default Queue Precedence	[1-8] Enter a precedence for the specified queue.
Default Queue Minimum Rate	[1-0 Kbps] The default minimum rate at which traffic can pass through the queue. [-1 Indicates no shaping.]
Default Queue Shaping Rate	[1-0 Kbps] The shaping rate for the specified queue. [-1 Indicates no shaping.]
Default Queue Shaping Burst Rate	[>= 1600] The maximum rate at which traffic can pass through the queue.

ETH Interface

Your gateway has four LAN ports. One of them can be re-purposed to become a WAN port when such an RJ45 WAN port is desired. After selecting **Advanced Setup** -> **Layer2 Interface** -> **ETH Interface** from the left navigation bar, click **Add** in the center pane. The following screen will appear. From the drop-down menu in the center pane, simply select the LAN port you wish to act as a WAN port.



WAN Service

There are several variations of WAN Service available to configure. The three core variations are:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

This chapter will illustrate a sample configuration scenario down each of these three variations and define the available fields to customize your WAN service setup.

PPP over Ethernet

After selecting **Advanced Setup** -> **WAN Service** from the left navigation bar, click the **Add** button. A progression of several screens will follow. Advance to the next after completing the required fields using the **Next** button appearing near the bottom of each screen.

First, select the Layer2 interface to use for the WAN service.

SMART/RG®
forward thinking

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)

Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0/(0_0_1)

Back Next

Click the **Next** button to advance to the next step.

Next, select the type of WAN service you wish to create. For this example choose PPP over Ethernet.

SMART/RG®
forward thinking

WAN Service Configuration

Select WAN service type:

☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

Enter Service Description: pppoe_0_0_1

Network Protocol Selection:
IPv4 Only

Back Next

Click **Next** after completing the necessary fields.

The individual fields on this screen are defined as follows:

Field Name	Description
WAN service type	[PPP over Ethernet PPPOE, IP over Ethernet IPoE, Bridging]
Enter Service Description	Enter a name to describe this configuration.
Network Protocol Selection	A data packet scheduling technique allowing different scheduling priorities to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (who has sent larger packets or more packets per second than the others since it became active) will only punish itself and not other sessions.

Next, configure the PPP Username, Password and related information.

Device Info

Advanced Setup

Layer2 Interface

ATM Interface

PTM Interface

ETH Interface

WAN Service

4G LTE Settings

Ethernet Config

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

DSL Bonding

UPnP

DNS Proxy

Interface Grouping

IP Tunnel

IPSec

Certificate

Multicast

Wireless

Diagnostics

Management

Logout

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method:

Link Control Protocol

LCP Keepalive Period (s):
 LCP Retry Threshold:

☐ PPP IP extension

☐ Advanced DMZ

Non DMZ IP Address:
 Non DMZ Net Mask:

☒ Use Static IPv4 Address

IPv4 Address:

☒ Retry PPP password on authentication error

Max PPP authentication retries (1-65536): (use 65536 to retry forever)

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

☒ Enable Firewall

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☒ Enable NAT

☐ Enable Fullcone NAT

☐ Enable SIP ALG

Multicast Proxy

☐ Enable IGMP Multicast Proxy

☐ No Multicast VLAN Filter

MTU size [1370-1492]:

☒ Use Base MAC Address on this WAN interface (Note: only select this for one WAN interface)

Click [Next](#) after completing the necessary fields.

The individual fields on this screen are defined as follows:

Field Name	Description
PPP Username:	Enter the Username required for authentication to the PPP server.
PPP Password:	Enter the Password required for authentication to the PPP server.
PPPoE Service Name:	(Optional) Enter a description for this service.
Authentication Method	Select a means for authentication from the drop-down list. [AUTO] Attempt to AUTO detect handshake protocol in list below. [PAP] Password Authentication Protocol (plaintext passwords) [CHAP] Challenge Handshake Authentication Protocol. (MD5 hashing scheme on passwords) [MSCHAP] Microsoft Challenge Handshake Authentication Protocol. (Microsoft encrypted password authentication protocol)
CP Keepalive Period	The frequency with which the keepalive packet is sent by the gateway to the PPP server.
LCP Retry Threshold	In the event that the PPP server does not respond to the Keepalive, how many additional attempted packets will the gateway send before giving up and declaring the connection, Failed.
Dial on Demand	[1-4320] Enables Inactivity Timeout (minutes). Default = 0 (not applicable.) Connection automatically starts when there is outbound traffic to the Internet. It automatically terminates if the connection is idle based on the value in the Idle Timeout setting.
PPP IP Extension	Forward all traffic to Advanced DMZ IP specified in the next field.
Advanced DMZ	Only applicable if PPP IP extension is selected. Specify IP to forward traffic PPPoE traffic to.
Use Static IPv4 Address	Specify IPv4 Address to apply to WAN service.
Retry PPP password on authentication error	[1-65536] Max PPP authentication retries on failure. (65536=Forever)
Enable PPP Debug Mode	The system will put more PPP connection information into the system log of the device. This is for debugging errors and not for normal usage.
Bridge PPPoE Frames Between WAN and Local Ports	PPPoE passthrough to relay PPPoE connections from behind the modem. Also known as Half-Bridged mode.
Enable Firewall	Enables functions in the Security sub-menu
Enable NAT	Enable sharing the WAN interface across multiple devices on the LAN. Also enables the functions in the NAT sub-menu and addition PPPoE NAT features to select.
-Enable Fullcone NAT	Enables what is known as one-to-one NAT. (Exposed when Enable NAT is checked.)
-Enable SIP	Enables Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications. (Exposed when Enable NAT is checked.)
Enable IGMP Multicast Proxy	Enables Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
No Multicast VLAN Filter	Disables multicast filtering between WAN and LAN (VlanMux) network.
MTU size	[1370-1492] Default=1492 bytes. Manually configure the MTU (Maximum Transmission Unit) size for SmartRG gateways supporting a gigabit-capable WAN interface. This value is expressed in bytes. This feature is supported by SmartRG models SR500n, SR505n, SR510n, SR550n and SR552n. Firmware v2.5.0.7 or later is required.

Field Name	Description
Use Base MAC Address on this WAN interface	Use SmartRG Devices Base (Primary) MAC address. When unchecked a unique MAC per service is assigned.
ADDITIONAL OPTIONS WHEN IPV4&IPV6 or IPV6 Only are selected at the WAN Service Creation Page	Enable IPv6 Unnumbered Model Enable IPv6 Unnumbered Model Launch Dhcp6c for Address Assignment (IANA) Launch Dhcp6c for Prefix Delegation (IAPD) Enable MLD Multicast Proxy

Next, Select the interface used as a default gateway used for the PPP service being created.

Use the -> button to move your highlighted selection from left to right or <- for right to left

Click **Next** after completing the necessary fields.

Select DNS Server Interface from available WAN interfaces.

Use the -> button to move your highlighted selection from left to right or <- to move your selection from right to left.

SMART/RG®

forward thinking

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0	-> ←-	

☐ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Alternatively, you may use the lower portion of the screen to manually key in static DNS IP addresses.

Click **Next** after completing the desired parameters.

Next, the summary screen will appear indicating that your PPPoE WAN setup is complete.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 1
Connection Type:	PPPoE
Service Name:	pppoe_0_0_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

Review the summary and either click Apply/Save to commit your changes or choose [Back](#) to step through this progression of screens in reverse order to make any necessary alterations you may desire.

IP Over Ethernet

The next WAN Service variant is IP over Ethernet.

After [selecting Advanced Setup -> WAN Service](#) from the left navigation bar, click the [Add](#) button. A progression of several screens will follow.

Advance to the next after completing the required fields using the [Next](#) button appearing near the bottom of each screen. First, select the Layer2 interface to use for the WAN service.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portid_vpi_vci)
For PTM interface, the descriptor string is (portid_high_low)
Where portid=0 --> DSL Latency PATH0
portid=1 --> DSL Latency PATH1
portid=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0/(0_0_1)

Back Next

Click the Next button to advance to the next step.

Next, select the type of WAN service you wish to create.

For this example choose **IP over Ethernet**.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service

WAN Service Configuration

Select WAN service type:

☐ PPP over Ethernet (PPPoE)
☒ IP over Ethernet
☐ Bridging

Enter Service Description: pppoe_0_0_1

Network Protocol Selection:
IPv4 Only

Back Next

Click **Next** after completing the necessary fields.

The individual fields on this screen are defined as follows:

Field Name	Description
WAN service type	[PPP over Ethernet PPPOE, IP over Ethernet IPoE, Bridging]
Enter Service Description	Enter a name to describe this configuration.
Network Selection	Protocol: [IPv4 Only] [IPv4&IPv6] (Dual Stack) "IPv4 and IPv6 running concurrently." [IPv6 Only] Note: When selecting IPv4&IPv6 or IPv6 the subsequent options presented will change accordingly.

Enter the relevant WAN IP Settings.

Click **Next** after completing the necessary fields.

The individual fields on this screen are defined as follows:

Field Name	Description
Obtain an IP address automatically	When you wish the ISP to automatically assign the WAN IP to the gateway.
Option 60 Vendor ID	(Optional) Broadcast a specific vendor ID for the DHCP server to accept the device.
Option 61 IAID	(Optional) Interface Association Identifier (IAID). A unique identifier for an IA, chosen by the client.
Option 61 DUID	(Optional) DHCP Unique Identifier (DUID) is used by the client to get an IP address from the DHCP server.

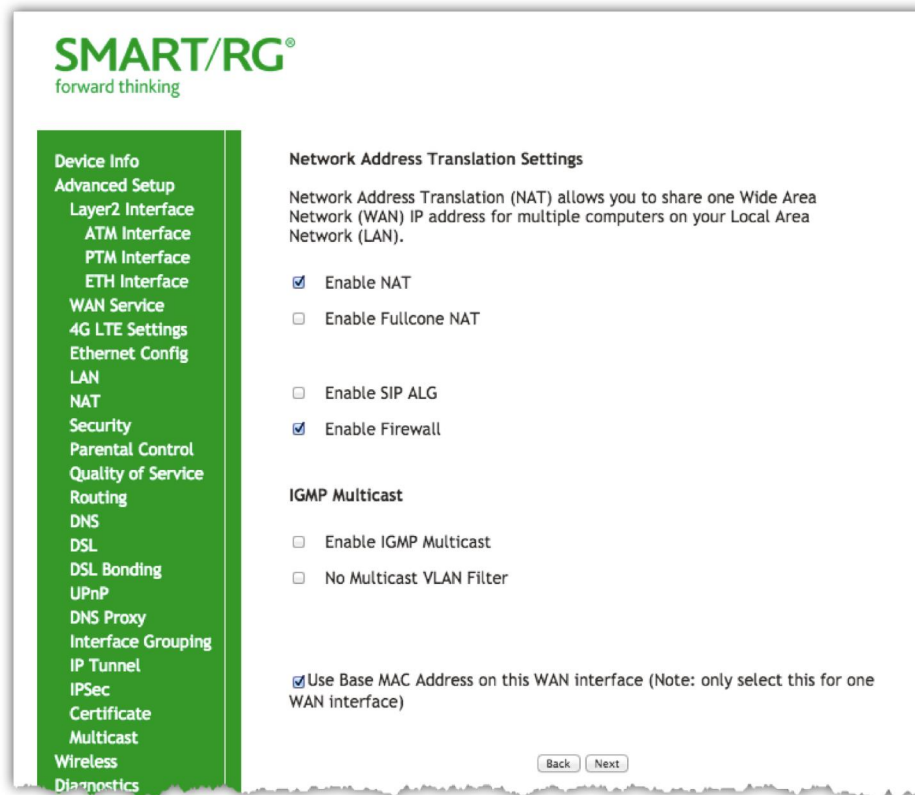
Field Name	Description
Use the following Static IP address	Use this section to manually declare the Static IP information provided by your ISP.
WAN IP Address	Enter the static WAN IPV4 Address.
WAN Subnet Mask	Enter the static Subnet Mask.
WAN gateway IP address	Enter the static Gateway IP address.
Advanced DMZ	(Optional) Check this option to enable Advanced DMZ on the WAN service.*
NON DMZ IP Address	(Optional) Broadcast a specific vendor ID for the DHCP server to accept the device.
NON DMZ Net Mask	Enter a secondary LAN IP address for the gateway. e.g. 192.168.2.1
Obtain an IPv6 address automatically	When you wish the ISP to automatically assign the WAN IP to the gateway.
Dhcpv6 Address Assignment (IANA)	Select this option for CPE to receive WAN IP from ISP.
Dhcpv6 Prefix Delegation (IAPD)	Select this option for CPE to generate WAN IP's prefix from server rest by MAC address.
Use the following Static IPv6 address	Use this section to manually declare v6 the Static IP information provided by your ISP.
WAN IPv6 Address/Prefix Length	Enter the IP address / prefix length
WAN Next-Hop IPv6 Address	Enter the IP address of

* For additional info see the SmartRG Support site's knowledgebase.

Next, scroll down and enter the NAT Settings.

No selections are required. All settings are optional.

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). If you do not want to enable NAT (atypical) and wish the user of this gateway to access the Internet normally, you need to add a route on the uplink equipment. Failure to do so will cause access to the Internet to fail.



The individual fields on this screen are defined as follows:

FIELD NAME	DESCRIPTION
Enable Firewall	Enables functions in the Security sub-menu
Enable NAT	Enable sharing the WAN interface across multiple devices on the LAN. Also enables the functions in the NAT sub-menu and addition PPPoE NAT features to select.
-Enable Fullcone NAT	Enables what is known as one-to-one NAT. (Exposed when Enable NAT is checked.)
-Enable SIP	Enables Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications. (Exposed when Enable NAT is checked.)
Enable IGMP Multicast Proxy	Enables Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
No Multicast VLAN Filter	Disables multicast filtering between WAN and LAN (VlanMux) network.
MTU size	[1370-1492] Default=1492 bytes. Manually configure the MTU (Maximum Transmission Unit) size for SmartRG gateways supporting a gigabit-capable WAN interface. This value is expressed in bytes. This feature is supported by SmartRG models SR500n, SR505n, SR510n, SR550n and SR552n. Firmware v2.5.0.7 or later is required.
Use Base MAC Address on this WAN interface	Use SmartRG Devices Base (Primary) MAC address. When unchecked a unique MAC per service is assigned.

Ethernet Config

Ethernet Port Configuration

Set the speed and duplex for each of the Ethernet ports.

After Selecting **Advanced Setup** -> **Ethernet Config** from the left navigation bar, make your selection from the Configure drop-down menu for each of the four Ethernet ports on your SmartRG gateway.

Select from Auto, 100 Full, 100 Half, 10 Full or 10 half. These options represent 100 megabit or 10 megabit using half or full duplex transmission protocols. Make a manual selection from one of the latter four options when you have a specific device with a known limited transmission speed capability. Simply choose Auto and your SmartRG gateway will automatically select an appropriate setting based on Ethernet auto negotiation with the NIC of the LAN host.

Model-specific variants:

- SR510, SR552n, SR500n The fourth port will be described in this screen as eth3/LAN1 and the ports are listed in reverse order. eth4/WAN interface is also present on these models.
- SR552n v2.5.0.6 and later has an additional selection available of 1000 Full for all Ethernet interfaces (shown below).
- SR505n v2.5.0.x and later has an additional selection available of 1000 Full for the LAN1/WAN port.

Click **Apply/Save** to commit your changes.

Port	Configure	Max Bit Rate	Duplex Mode	Status
eth0/LAN4	Auto	1000	Full	Down
eth1/LAN3	Auto	1000	Full	Down
eth2/LAN2	Auto	1000	Full	Down
eth3/LAN1	Auto	1000	Full	Down
eth4/WAN	Auto	1000	Full	Up

Save/Apply

LAN

Local Area Network (LAN) Setup

Utilize this screen to configure the router's local IP addresses, subnet mask, DHCP behavior and other related LAN side settings for your SmartRG Gateway.

After selecting **Advanced Setup** -> **LAN** from the left navigation bar, customize the fields as desired.

Click [Apply/Save](#) to commit your changes.

SMART/RG®
forward thinking

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default ▾

IP Address:
Subnet Mask:

☒ Enable IGMP Proxy
☒ Enable IGMP Snooping

☐ Standard Mode
☒ Blocking Mode

☐ Enable LAN side firewall

☐ Disable DHCP Server
☒ Enable DHCP Server

Start IP Address:
End IP Address:
Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
Add Entries Remove Entries		

Automatically create static IP leases for the following OUIs:

OUI	Remove
Add OUI Remove OUI	

Configure DHCP Options:

Option 66: (TFTP Server Name)
Option 150: (Comma-separated list of TFTP Server IPv4 Address(es) (maximum 2 entries))

☒ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:
Subnet Mask:

[Apply/Save](#)

The individual fields on this screen are defined as follows:

Field Name	Description
Groupname	From the drop-down list, select from the available groupings of interfaces as defined via the Interface Grouping screen.
IP Address	Set the LAN IP address by which LAN devices will connect to this gateway.
Subnet Mask	Set the Subnet mask to be used by LAN devices connecting to this gateway.
Enable IGMP Snooping	Enable your SmartRG gateway to listen to Internet Group Management Protocol (IGMP) network traffic between hosts and routers. By listening to these conversations the gateway maintains a map of which links need which IP multicast streams.

Field Name	Description
Standard Mode	When selected, multicast traffic will flood to all bridge ports when there is no client subscribed to any multicast group.
Blocking Mode	When selected, multicast data traffic will be blocked and not flood to all bridge ports when no client subscriptions to a multicast group are present.
Enable LAN Side Firewall	Enable the restriction of traffic between LAN hosts.
Enable / Disable DHCP Server	The Dynamic Host Control Protocol Server (DHCP) functionality of your SmartRG gateway will automatically assign LAN IP addresses to host devices as they connect with the gateway. Select Enable DHCP Server to take advantage of this feature.
Start IP Address	Enter the beginning of the class C, IP address range to be assigned by the DHCP server.
End IP Address	Enter the end of the class C, IP address range to be assigned by the DHCP server.
Lease Time (Hour)	Set the number of hours for which an IP address will be leased.
Static IP Lease List	Click the Add Entries button to enter a literal, static, IP address to be associated with a specific MAC Address of one of your LAN host devices. Click Apply/Save when done. Additional entries may be created. Click the Add Entries button to enter the OUI of one of your LAN host devices for which it is desired that the gateway assign a static IP. Click Apply/Save when done. Additional entries may be created.
Automatically create static IP leases from the following OUIs DHCP Option 66 (TFTP Server Name)	For LAN hosts, IP addresses can be assigned manually or by using DHCP. For some devices that also require access to a TFTP server (contains device configuration name files in .cnf file format), which enables the device to communicate with other infrastructure, select this option to specify the name of the TFTP server. Option 66 is an IEEE standard.
DHCP Option 150 (comma-separated list of TFTP server IPv4 Address(es))	A Cisco proprietary methodology for pointing to a TFTP server. Unlike Option 66, Cisco's Option 150 supports a list of TFTP server's IP addresses. Max 2 entries.
Enable DHCP Server Relay	The DHCP relay agent operates as the interface between DHCP clients and the server. It listens for client requests and adds vital configuration data, such as the client's link information, which is needed by the server to allocate the address for the client. When the DHCP server responds, the DHCP relay agent forwards the reply back to the DHCP client.
DHCP Server IP Address	Set the IP address to which LAN clients must connect to receive DHCP services.
Configure the second IP address and subnet mask for LAN interface	When selected, additional fields are exposed that enable the declaration of a second IP address and Subnet mask to support a second, simultaneous LAN. i.e. the primary LAN defined above may be at 192.168.0.1 and this secondary LAN may be defined as 192.168.2.1.

IPv6 Autoconfig

Utilize this screen to establish your Gateway's IPv6 environment.

After selecting [Advanced Setup -> LAN -> IPv6 Autoconfig](#) from the left navigation bar, customize the fields as desired.

Click [Apply/Save](#) to commit your changes.



Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
IPv6 Autoconfig
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☒ Enable DHCPv6 Server

☒ Stateless
☐ Stateful

Start interface ID:
End interface ID:
Leased Time (hour):

☒ Enable RADVD

☐ Enable ULA Prefix Advertisement
☐ Randomly Generate
☒ Statically Configure

Prefix:
Preferred Life Time (hour):
Valid Life Time (hour):

☒ Enable MLD Snooping

☐ Standard Mode
☒ Blocking Mode

Save/Apply

Field Name	Description
Interface Address (prefix length is required)	IPv6 address to assign as the gateways Local LAN IPV6 address and prefix length.
Enable DHCP v6 Server	Check this option to turn on the DHCP v6 feature on the LAN.
Enable DHCP Server - Stateless	Inherit IPv6 address assignments from the WAN IPV6 interface.
Enable DHCP Server - Stateful	DHCPv6 server given by the LAN IPV6 network as configured with additional options. Start interface ID: Enter the beginning IPv6 available addresses for DHCP to assign to LAN devices. End interface ID: Enter the ending IPv6 available addresses for DHCP to assign to LAN devices. Leased Time (hour): Amount of time before a new IPv6 lease is requested by the LAN client.

Field Name	Description
Enable RADVD	(Optional) Router Advertisement Daemon (RADVD) service that sends router advertisements to LAN clients. Enable ULA Prefix Advertisement- Check this option to enable unique local address (ULA) advertisement on the LAN. Randomly Generate- Select this option to enable the gateway to generate a random IPv6 prefix.
Enable MLD Snooping	(Optional) Multicast Listener Discovery (MLD) snooping manages the IPV6 multicast traffic. Standard Mode: Multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if IGMP snooping is enabled. Blocking Mode: The multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

NAT

Virtual Servers (Port Forward)

Virtual Servers (more commonly known as Port Forward) is a technique used to facilitate communications by external hosts with services provided within a private local area network.

After Selecting **Advanced Setup** -> **NAT** -> **Virtual Servers** from the left navigation bar, click the Add button. The following screen will appear. Customize the fields to create your port forwarding entry.

Click **Apply/Save** to commit your changes.

SMART/RG®
forward thinking

Device Info

Advanced Setup

Layer2 Interface

WAN Service

4G LTE Settings

Ethernet Config

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

Security

Parental Control

Quality of Service

Routing

DNS

DSL

DSL Bonding

UPnP

DNS Proxy

Interface Grouping

IP Tunnel

IPSec

Certificate

Multicast

Wireless

Diagnostics

Management

Logout

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.

NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured:96

Use Interface

pppoe_0_0_1/ppp0

Service Name:

☒ Select a Service:

Select One

☐ Custom Service:

Server IP Address:

192.168.1.

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Use Interface	Select the WAN interface that this NAT rule will apply to.
Select a Service	Select from a list of common applications that typically require port forwards in place. The port ranges and protocol fields will be pre-populated
Custom Service	If your application does not appear in the preceding drop-down list you may manually enter a unique name for the application.
Server IP Address	IP address of the LAN client in which the service has been hosted.
External Port Start	External Port to start with
External Port End	External Port to end with
Protocol	Protocol used Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) or TCP/UDP
Internal Port Start	Internal Port to start with
Internal Port End	Internal Port to end with

Port Triggering

Some applications require that specific ports in the gateway's firewall be opened for access by remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the [Triggering Ports](#). The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the [Open Ports](#).

After selecting [Advanced Setup -> NAT -> Port Triggering](#) from the left navigation bar, click the Add button. Customize the fields as needed for the firewall pinholes you wish to establish. A maximum 96 entries can be configured.

Click [Apply/Save](#) to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.
Remaining number of entries that can be configured: 96

Use Interface:

Application Name:
☒ Select an application:
☐ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

The individual fields on this screen are defined as follows:

Field Name	Description
Use Interface	Select the interface over which the port triggering rule will apply.
Select an Application	Choose from this list of applications which commonly require a Port trigger entry.
Custom Application	A free form text field. Enter a unique name for the application for which you are creating a Port Trigger entry
Trigger Port Start	[1-65535] An outgoing trigger port number. Set the beginning of the range of available ports.
Trigger Port End	[1-65535] An outgoing trigger port number. Set the end of the range of available ports.
Trigger Protocol	[TCP, UDP, TCP/UDP] Select the protocol required by the application that will be using the ports in the specified range.
Open Port Start	[1-65535] An incoming port number. Set the beginning of the range of available ports.
Open Port End	[1-65535] An incoming port number. Set the end of the range of available ports.
Open Protocol	[TCP, UDP, TCP/UDP] Select the protocol from the drop down list.

DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer. If it is desired to route all internet traffic with no filtering or security to a specific LAN device, add the IP address of that device to this field.

After selecting **Advanced Setup -> NAT -> DMZ Host** from the left navigation bar, enter the DMZ Host IP Address.

Click **Apply/Save** to commit the new or changed address.

The screenshot shows the SMART/RG web interface. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Virtual Servers, Port Triggering, and DMZ Host (which is highlighted). The main content area is titled "NAT -- DMZ Host". It contains the following text: "The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer." Below this, it says: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." There is a text input field labeled "DMZ Host IP Address:" and a "Save/Apply" button at the bottom right.

Security

IP Filtering - Outgoing

Add an Outgoing filter when refusal of data from the LAN to the WAN is desired.

After selecting **Advanced Setup -> Security -> IP Filtering -> Outgoing** from the left navigation bar, click the Add button. The following screen will appear to facilitate the filtering you desire. Click **Apply/Save** to commit the completed entry.

The screenshot shows the SMART/RG web interface. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Security, IP Filtering, Outgoing (which is highlighted), Incoming, MAC Filtering, Parental Control, DNS, and DSL. The main content area is titled "Add IP Filter -- Outgoing". It contains the following text: "The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter." Below this, there are several fields: "Filter Name:" with a text input field, "IP Version:" with a dropdown menu showing "IPv4", "Protocol:" with a dropdown menu, "Source IP address[/prefix length]:" with a text input field, "Source Port (port or port:port):" with a text input field, "Destination IP address[/prefix length]:" with a text input field, and "Destination Port (port or port:port):" with a text input field. There is an "Apply/Save" button at the bottom right.

The individual fields on this screen are defined as follows:

Field Name	Description
Filter Name	A free form text field. Give your filter an intuitive name.
IP Version	Version IPv4 is selected by default. IPV6 can be alternately selected. For the filter to be IPV6 configured and effective requires the gateway be installed on a network that is either a pure IPV6 network having that protocol enabled or it is both IPV4 and IPV6 dual protocol enabled/configured. Choosing IPV6 means both the Source and Destination IP address as described below must be specified in IPV6 format (e.g. the following is an IPV6 compliant, hexadecimal address. 2001:0DB8:AC10:FE01:0000:0000:0000:0001).
Protocol	[TCP/UDP,TCP, UDP, or ICMP] Sets the protocol profile for the filter you are defining. TCP/UDP is most commonly used.
Source IP address [/prefix length]	Enter the source IP address of a LAN side host for which you wish to filter/block it's outgoing traffic for the specified protocol(s).
	NOTE: The address specified here can be a particular address or a block of IP address on a given network subnet. This is done through appending the address with the routing " /prefix " length decimal value (preceded with the slash) associated. Use of a valid decimal routing prefix for defining the subnet mask per CIDR notation is required).
Source Port (port or port:port)	Set the outgoing host port (or range of ports) for the above host (or range of hosts defined by optional routing " /prefix " subnet mask) to define the ports profile for which egress traffic will be filtered from reaching the specified destination(s).
Destination IP address	Enter the source IP address of a LAN side host for which you wish to filter/block it's outgoing traffic for the specified protocol(s). Note: The address specified here can be a particular address or a block of IP address on a given network subnet. This is done through appending the address with the routing " /prefix " length decimal value (preceded with the slash) associated. Use of a valid decimal routing prefix for defining the subnet mask per CIDR notation is required).
Destination Port (port or port:port)	Set the destination host port (or range of ports) for the above host (or range of hosts defined by optional routing " /prefix " subnet mask) to define the destination ports profile for which the filtered host egress traffic will be filtered from reaching the otherwise intended destination(s) (e.g. to block the traffic to those ports on, say, a computer external to the local network.)

IP Filtering - Incoming

Add an Incoming filter when refusal of data from the WAN to the LAN is desired.

After selecting **Advanced Setup -> Security -> IP Filtering -> Incoming** click the **Add** button. The following screen will appear to facilitate the filtering you desire. Click **Apply/Save** to commit the completed entry.

The individual fields on this screen are defined as follows:

Field Name	Description
Filter Name	A free-form text field. Enter a descriptive name for this filter.
IP Version	Version IPv4 applies by default. IPV6 can be alternately selected.
Protocol	[TCP/UDP, TCP, UDP, or ICMP] Select the protocol to be associated with this incoming filter.
Source IP address [/prefix length]	Enter source address for rule.
Source Port (port or port:port)	Enter source port number or range. (Destination port numbers xxxxx:yyyyy).
Select All checkbox	Check as applicable to apply rule to all interfaces.
First WAN interface (e.g. pppoe based) checkbox	Check each as applicable to effect rule on specific WAN interface(s). WAN interface (s) available for selection will be those configured in Routing mode and with firewall enabled.
Last WAN interface (e.g. ipoe based) checkbox	
First LAN interface checkbox	Check each as applicable for desired rule.
Second LAN interface (as applicable) checkbox	
Bridged Interface checkbox	Check as applicable for desired rule.

MAC Filtering

Your SmartRG gateway can block or forward packets based on the originating device. This MAC filtering feature is available only in Bridging mode. For other modes, similar functionality is available via IP Filtering.

After selecting **Advanced Setup -> Security -> MAC Filtering** from the left sidebar, alter the Policy to **FORWARD** or **BLOCKED** as desired.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode.
FORWARDED means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table.
BLOCKED means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
ptm0	FORWARD	☐

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

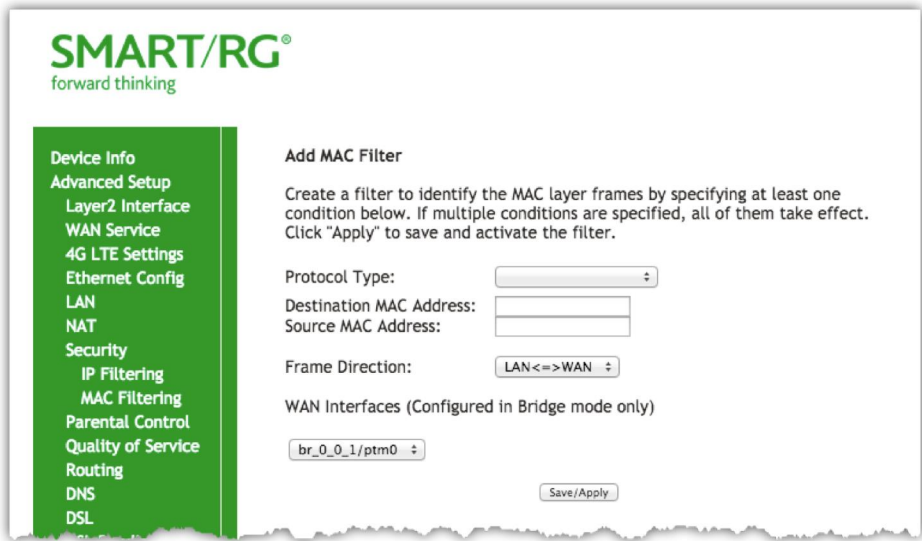
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

[Add](#) [Remove](#)

The individual fields on this screen are defined as follows:

Field Name	Description
Interface	Interface(s) associated with established policy rule(s).
Policy	[FORWARD, BLOCKED] The current/active policy type that is in place.
Change	Check this box then click the Change Policy button to toggle the policy type.

Next, click the **Add** button. The following screen will appear.
 Click **Apply/Save** to commit the changes.



The individual fields on this screen are defined as follows:

Field Name	Description
Protocol Type	[PPPoE, IPv4/IPv6, AppleTalk, IPX, NetBEUI, IGMP] Select the protocol associated with the device at the destination MAC address.
Destination MAC Address	Enter the MAC address of the hardware you wish to associate with this filter.
Source MAC Address	Enter the MAC address of the device that is originating requests intended for the device associated with the Destination MAC address.
Frame Direction	Select the incoming/outgoing packet interface.
WAN Interfaces	Applies the filter to the selected interface(s).

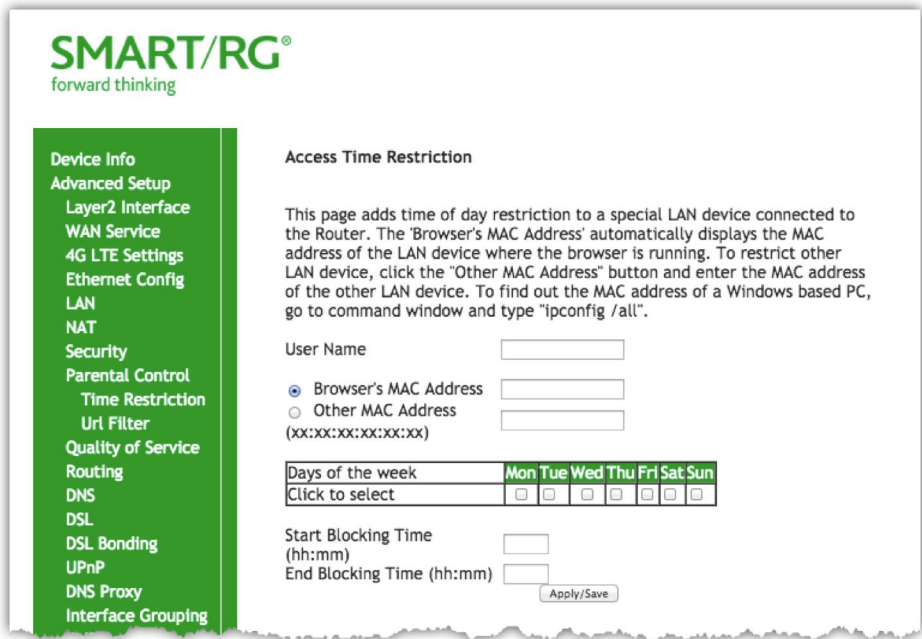
Parental Control

The Parental Control features of your SmartRG gateway enable restriction of Internet access on a LAN host by LAN host basis. This is achieved without the need for client software to be installed on each host.

Time Restriction

Time Restriction features can be established on a per MAC address basis for individual LAN hosts. Access constraints by day of week and time of day are available to customize per the preferences of the subscriber.

After selecting **Advanced Setup -> Parental Control -> Time Restriction**, click the **Add** button toward the center. The following screen will appear:



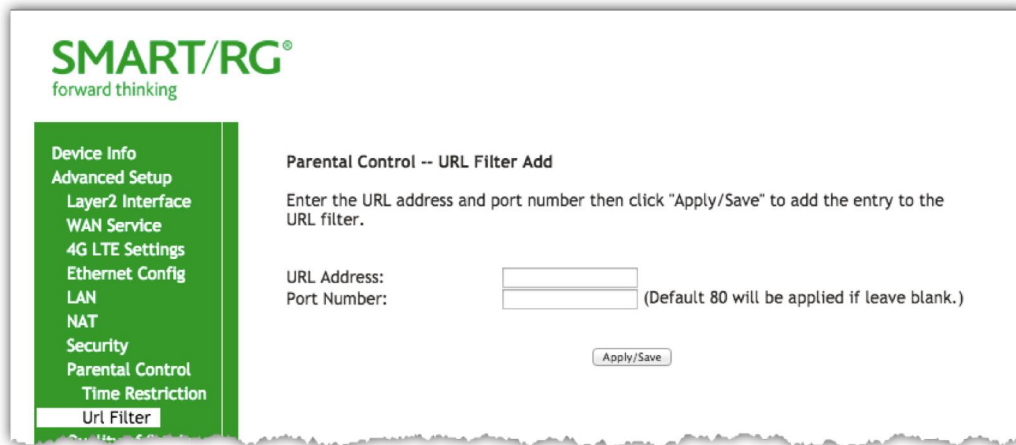
The individual fields on this screen are defined as follows:

Field Name	Description
User Name	A free form text field. Enter and intuitive name for this restriction.
Browser's MAC Address	MAC address of the PC to which this restriction will uniquely apply.
Other MAC Address (xx:xx:xx:xx:xx:xx)	MAC address of another LAN device to restrict.
Days of the week	Check the box(es) for day(s) Mon - Sun the restrictions apply.
Start Time Blocking / End Time Blocking	Enter the range of time that the above stated device(s) is to be restricted from access to the Internet.

URL Filter

The other side of the Parental Controls coin is URL filtering. From the left navigation bar, select **Advanced Setup -> Parental Control -> Url Filter**. Choose the **Exclude List** radio button to add a URL to be blocked. Note that the **Include List** is a feature of Cisco Prime Home™ Plus and is only supported when the gateway is under management by Cisco Prime Home™. In that event, these settings must be applied via the, "Content Filtering" features Cisco Prime Home™ and not from this native, gateway user interface.

Next click the **Add** button toward the center of the screen. The following screen will appear:



Note that there is only one **Block List** and one **Allow List** per gateway. The stand-alone modem capability does not maintain a unique Allow and Block List for each individual LAN device. Some additional flexibility however is available when your SmartRG gateway is under management of Cisco Prime Home™. Refer to Cisco documentation regarding, "Content Filtering" for instructions.

The individual fields on this screen are defined as follows:

Field Name	Description
URL Address	URL address to be added to the enabled applicable Exclude or Include list.
Port Number	Port number associated with URL being added (default 80).

Quality Of Service

QoS enables prioritization of internet content to help ensure the best possible performance. This is particularly useful for streaming video and audio content to minimized potential for drop-outs. QoS becomes significant when the sum of the traffic (audio, video, data) exceeds the capacity of the line.

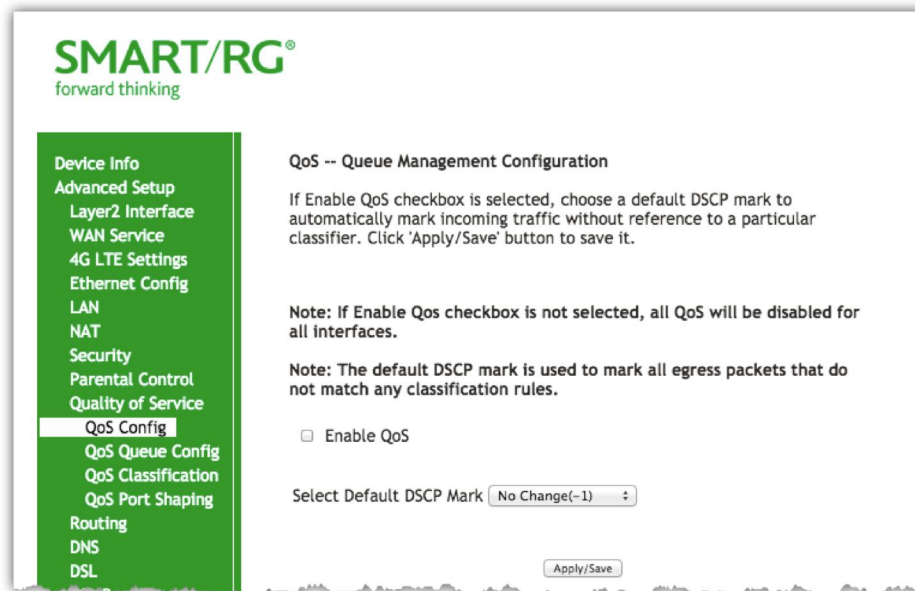
QoS Config

Use the QoS Config screen to enable QoS and set the **DSCP Mark classification**.

NOTE:

- In ATM mode, the maximum queues that can be configured is 16.
- In PTM mode, the maximum queues that can be configured is 8.
- For each Ethernet interface, the maximum configurable queues is 4.
- Queues for Wireless (e.g. WMM Voice Priority for wl0 interface) show only when wireless is enabled. If the WMM Advertise function in the Wireless Basic Setup page is disabled, classification related to wireless will have no effect.

After selecting **Advanced Setup -> Quality Of Service -> QoS Config**, click the checkbox toward the center of the screen if you wish to enable QoS.



When this option is checked, it exposes the QoS Queue Management Configuration drop-down menu where selection of the default Differentiated Services Code Point (DSCP) Mark classification value to be associated can be declared.

If this option was already enabled and the check is removed, QoS for ALL interfaces will be turned off upon clicking [Apply/Save](#).

For a commonly used DSCP values refer to RFC 2475.

Your SmartRG gateway makes available the following values:

No Change(-1)	AF22(010100)	AF43(100110)
Auto Marking(-2)	AF21(010010)	AF42(100100)
Default(000000)	CS2(010000)	AF41(100010)
AF13(001110)	CS2(010000)	CS4(100000)
AF12(001100)	AF33(011110)	EF(101110)
AF11(001010)	AF32(011100)	CS5(101000)
CS1(001000)	AF31(011010)	CS6(110000)
AF23(010110)	CS3(011000)	CS7(111000)

Click to [Apply/Save](#) to commit the changes.

QoS Queue Management Configuration marking on ingress packets in accordance with the [Select Default DSCP Mark](#) setting field just above it. Queue management on ingress packets will mark according to the highlighted selection therein. The associated default marking will then automatically be applied to all incoming packets without reference to a particular classification.

NOTE: An default DSCP Mark of value Default(000000) will mark all egress packets that do NOT match any classification.

QoS Queue Config

Use the **QoS Queue Config** to configure a queue and add it to a selected Layer2 interface.

After selecting **Advanced Setup -> Quality Of Service -> QoS Queue Config**, click the button. The following screen will appear to facilitate the creation of a queue and associate it with an interface.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
QoS Config
QoS Queue Config
QoS Classification
QoS Port Shaping
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate

QoS -- Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

(Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.)

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

Minimum Rate: [1-100000 Kbps] (-1 indicates no shaping)
Shaping Rate: [1-100000 Kbps] (-1 indicates no shaping)
Shaping Burst Size: [bytes] (shall be >=1600)

The individual fields on this screen are defined as follows:

Field Name	Description
Name	A free form text field. Enter an intuitive name for your config.
Enable	Dropdown selection for either enable or disable of a given QoS queue configured on chosen Layer 2 interface. Note: Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.
Interface	Dropdown selection for desired Layer 2 interface to be associated with the defined QoS queue (e.g. eth0, eth4). The following selections are exposed upon defining an Interface as described above:
Queue Precedence	Dropdown selection for priority value to be associated with QoS queue defined (e.g. 1(SP), 2(SP), 3(SP), 4(SP WRR WFQ)). Note: Lower value = higher priority The following selections are exposed only if SP WRR WFQ Queue Precedence priority as defined above is selected.

Field Name	Description
Scheduler Algorithm	Algorithms for data priority in queue: [Strict Priority] Allows shaping of rate and burst size for packets in queue. [Weighted Round Robin] Applies a fair round robin scheme weighting effective for e.g. ATM networks with fixed packets size. [Weighted Fair Queuing] Applies a fair queuing weighting scheme via allowing different sessions to have different service shares for improved data packets flow in networks with variable packets size e.g. PTM/IP networks.
The following selections are exposed only if Strict Priority is selected as Scheduler Algorithm with Queue Precedence of SP WRR WFQ.	
Minimum Rate	[1-100000 Kbps] [-1 value indicates no minimum shaping applied] Minimum shaping rate defined for packets in QoS queue.
Shaping Rate	[1-100000 Kbps] [-1 value indicates no minimum shaping applied] Shaping rate defined for packets in QoS queue defined.
Shaping Burst Size	[1600 bytes or greater] Shaping defining specific burst size to be applicable to packets in queue defined.
The following selections are exposed if either Weighted Priority algorithm is selected as Scheduler Algorithm.	
Minimum Rate	[1-100000 Kbps] [-1 value indicates no minimum shaping applied] Minimum shaping rate defined for packets in QoS queue.
Shaping Rate	[1-100000 Kbps] [-1 value indicates no minimum shaping applied] Shaping rate defined for packets in QoS queue defined.

QoS Classification

Use **QoS Classification** to create traffic class rule to classify the ingress traffic into a priority queue. Optionally, you may also mark the DSCP or Ethernet priority of the packet.

After selecting **Advanced Setup -> Quality Of Service -> QoS Classification**, click the **Add** button. The following screen will appear. A maximum of 32 entries can be configured.

Click the **Apply/Save** button to commit your changes.

The individual fields on this screen are defined as follows:

Field Name	Description
Classification Name	A free form text field. Enter a descriptive name for this rule.
Rule Order	[Last, Null] Select Last to set this rule as the very last classification rule to be processed. Select Null to set this rule as the next classification rule to be processed within the existing list of classification rules.
Rule Status	[Enable, Disable] Select whether this rule is active or turned off.
Class Interface	[local, eth0..eth4, wl0] Select an interface.
Ether Type	[IP, ARP, IPV6] Select the Ethernet interface type for this classification.
Source MAC Address Source MAC Mask	Enter the source MAC Address and Source MAC Mask applied to classification.

Field Name	Description
Destination MAC Address Destination MAC Mask	Enter the destination MAC Address and destination MAC Mask applied to classification.
Source IP Address/Mask	Enter the source IP Address and Source IP Mask applied to classification.
Protocol	(Optional) Enter the Protocol specified for classification criteria.
UDP/TCP Source Port	(Optional) Enter the Source Port applicable for classification criteria. Expressed as a range or single port. (port:port or port).
UDP/TCP Destination Port	(Optional) Enter the Destination Port applicable for classification criteria. Expressed as a range or single port. (port:port or port).
Specify Class Queue	Choose from available queues in the drop-down list. Packets classified into a queue that exit through an interface for which a queue is not specified to exist, will instead egress to the default queue on the interface.
Mark Differentiated Code Point	Applied Service: Select the desired DSCP code from the drop down list.
802.1P priority	[1-7] (Lower values have higher priority.) This value is inserted into the Ethernet frame to be used by QoS disciplines to differentiate traffic.
Rate Limit (kbps)	Data traffic rate limit applied to classification.

QoS Port Shaping

QoS Port Shaping facilitates setting a fixed rate (Kbps) for each of the Ethernet ports.

Select [Advanced Setup](#) -> [Quality Of Service](#) -> [QoS Port Shaping](#) and the following screen will appear.

Click the [Apply/Save](#) button to commit the changes entered.



forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
QoS Config
QoS Queue Config
QoS Classification
QoS Port Shaping
Routing

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate (Kbps)	Burst Size (bytes)
eth3	LAN	-1	0
eth2	LAN	-1	0
eth1	LAN	-1	0
eth0	LAN	-1	0
eth4	LAN	-1	0

[Apply/Save](#)

The individual fields on this screen are defined as follows:

Field Name	Description
Interface	Each line item in the table represents one of the Ethernet LAN ports on the back of your SmartRG gateway.
Type	[LAN, WAN] Describes the function for which each physical port is configured on the gateway.
Shaping Rate (Kbps)	[1 - 1,000,000 Kbps] Sets the data rate for packets on the specified Interface.
Burst Size (bytes)	A value of -1 indicates no shaping. "Burst Size" will be ignored.

Routing

Default Gateway

Select **Advanced Setup** -> **Routing** -> **Default Gateway** and the following screen will appear.

Use the -> button to move your highlighted selection from left to right or <- for right to left.

Click the **Apply/Save** button to commit the changes entered.

The individual fields on this screen are defined as follows:

Field Name	Description
Available Routed WAN Interfaces	Choose from the list of available WAN interfaces identify as the Default Gateway.
Selected Default Gateway Interfaces	When populated, this becomes a prioritized list of Default Gateways selections.
Selected WAN Interface	Select the WAN interface for this route from the drop-down list. (NO CONFIGURED INTERFACE is default)

Static Route

Static Route is one form of manually configured, fixed route for IP data.

After selecting [Advanced Setup -> Routing -> Static Route](#), click the [Add](#) button and the following screen will appear. Click the [Apply/Save](#) button to commit the changes entered.

Up to 32 entries may be added.

The individual fields on this screen are defined as follows:

Field Name	Description
IP Version	[IPv4, IPv6] Select the IP version associated with the static route you wish to create.
Destination IP address/prefix length	Enter the destination network address / subnet mask for route
Interface	WAN Interface(s) available for selection. This list filtered by to IP Version set in the first drop-down list.
Gateway IP Address	Destination IP address desired (/prefix length if needed)
Metric (optional)	[>=0] Establishes traffic priority/weighting.

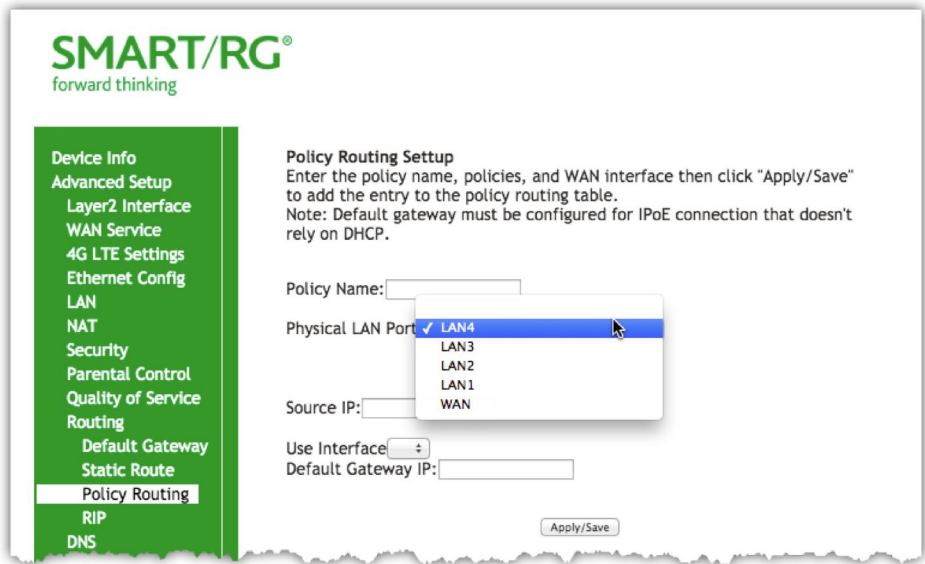
Policy Routing

Policy routing makes somewhat automated routing choices based on net admin dictated policies. For example, a network administrator might want to deviate from standard routing based on destination markers in the packet and instead, forward a packet based on the source address. Use

this feature to establish similar policies.

After selecting [Advanced Setup -> Routing -> Policy Route](#), click the [Add](#) button and the following screen will appear.

Click the [Apply/Save](#) button to commit the changes entered.



The individual fields on this screen are defined as follows:

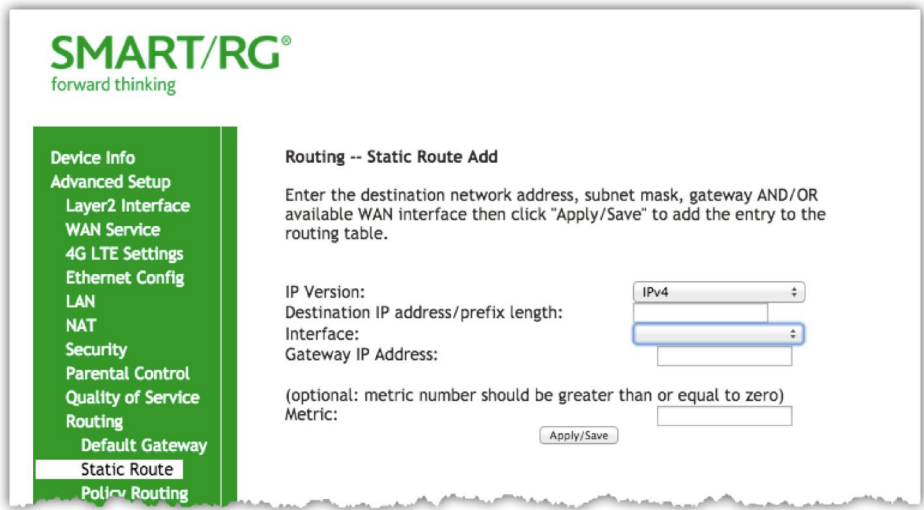
Field Name	Description
Policy Name	A free-form text field. Enter a descriptive name for this entry to the policy routing table.
Physical LAN Port	Select a physical LAN interface for the policy route from the drop-down list.
Source IP	Enter the IP address for source of this policy route.
Use Interface	Drop-down field selection providing choice of the WAN Interface desired for the policy route
Default Gateway IP	The IP address of the Default Gateway.

RIP (Routing Information Protocol)

RIP is a type of distance-vector routing protocol, which leverages hop count as a metric for routing. RIP puts a limit on the number of hops (max 15) allowed in order to prevent routing loops. This can sometimes limit the size of networks that RIP can be successfully employed.

After selecting [Advanced Setup -> Routing -> RIP](#), click the [Add](#) button and the following screen will appear.

Click the [Apply/Save](#) button to commit the changes entered.



The individual fields on this screen are defined as follows:

Field Name	Description
Interface	This column shows a list of available WAN interfaces. Complete the line item(s) associated with the interface you wish to employ RIP.
Version	[1,2,Both] Select the version of Routing Interface Protocol you desire. Reference RFC 1058 and RFC 1453 for detailed information on RIP versions.
Operation	[Passive, Active] Passive mode listens only. It does not advertise routes. Select Active mode to both listen and advertise routes.
Enabled	Check this box to employ RIP on the displayed interface.

DNS

DNS Server

Use the features of this screen to input the Domain Name Server information supplied by the service provider.

After selecting **Advanced Setup -> DNS -> DNS Server** from the left navigation bar, the following screen will appear.

Enter your desired settings. Click **Apply/Save** to commit changes.

SMART/RG®

forward thinking

Device Info

Advanced Setup

Layer2 Interface

WAN Service

4G LTE Settings

Ethernet Config

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DNS Server

Dynamic DNS

Static DNS

DSL

DSL Bonding

UPnP

DNS Proxy

Interface Grouping

IP Tunnel

IPSec

Certificate

Multicast

Wireless

Diagnostics

Management

Logout

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☐ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

->

<-

☒ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Select the configured WAN interface for the IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for the IPv6 DNS server will enable the DHCPv6 Client on that interface.

☐ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

☒ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

The individual fields on this screen are defined as follows:

Field Name	Description
Selected DNS Server Interfaces	The WAN service selected to be your primary DNS server.
Available Wan Interfaces	WAN services available to be selected for the DNS server.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server.
WAN Interface Selected	Alter this field only if IPv6 environment.
Primary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.
Secondary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.

Dynamic DNS

Dynamic DNS (DDNS) automatically updates a name server in the DNS with the active DNS configuration of its configured hostnames, addresses or other data. Often this update occurs in real time.

After selecting **Advanced Setup -> DNS -> Dynamic DNS** from the left navigation bar, click the **Add** button. The following screen will appear.

Enter your desired settings then click **Apply/Save** to commit your changes.

The individual fields on this screen are defined as follows:

Field Name	Description
D-DNS provider	Select a dynamic Domain Name Server provider from the drop-down menu.
Hostname	Enter the name of the dynamic DNS server.
Interface	Select the gateway WAN interface whose traffic will be pointed at the above specified Dynamic DNS provider
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

Static DNS

The Static DNS service allows you to resolve DNS queries on the Broadband Router by adding static Host Name to IP Address mappings.

After selecting **Advanced Setup -> DNS -> Static DNS** from the left navigation bar, click the **Add** button. The following screen will appear.

Enter your desired settings then click **Apply/Save** to commit your changes.

A maximum of 10 static DNS entries can be added.



The individual fields on this screen are defined as follows:

Field Name	Description
Hostname	Enter the hostname of the client computer.
Interface	Enter the IP address of the DNS server client uses to assist in resolving domain names.

DSL

Advanced settings for the DSL interface.

CAUTION: Altering these settings unnecessarily could result in the gateway being unable to attain DSL synchronization.

After selecting **Advanced Setup** -> **DSL** from the left navigation bar, click the **Add** button. The following screen will appear.

Enter your desired settings then click **Apply/Save** to commit your changes.

SMART/RG®

forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

DSL Settings

Select the modulation below.

☒ G.Dmt Enabled
☒ G.lite Enabled
☒ T1.413 Enabled
☒ ADSL2 Enabled
☒ AnnexL Enabled
☒ ADSL2+ Enabled
☐ AnnexM Enabled
☒ VDSL2 Enabled

Select the profile below.

☒ 8a Enabled
☒ 8b Enabled
☒ 8c Enabled
☒ 8d Enabled
☒ 12a Enabled
☒ 12b Enabled
☒ 17a Enabled

US0

☒ Enabled

Select the phone line pair below.

☒ Inner pair
☐ Outer pair

Capability

☒ Bitswap Enable
☐ SRA Enable
☐ PhyR Enable
☐ ADSL PTM Mode Enable

Inventory Management

☐ Use board serial for EOC Serial Number

Apply/Save

Advanced Settings

The individual fields on this screen are defined as follows:

Modulation	Data Transmission Rate
G.Dmt	ITU-T G.992.1 standard. Max Downstream: 12 Mbps Max Upstream: 1.3 Mbps
G.lite	ITU-T G.991.2 standard. Max Downstream: 4 Mbps Max Upstream: 0.5 Mbps
T1.413	ANSI T1.413 Issue 2 standard Max Downstream: 8 Mbps Max Upstream: 1.0 Mbps
ADSL2	ITU-T G.992.3 standard. Max Downstream: 12 Mbps Max Upstream: 1.0 Mbps

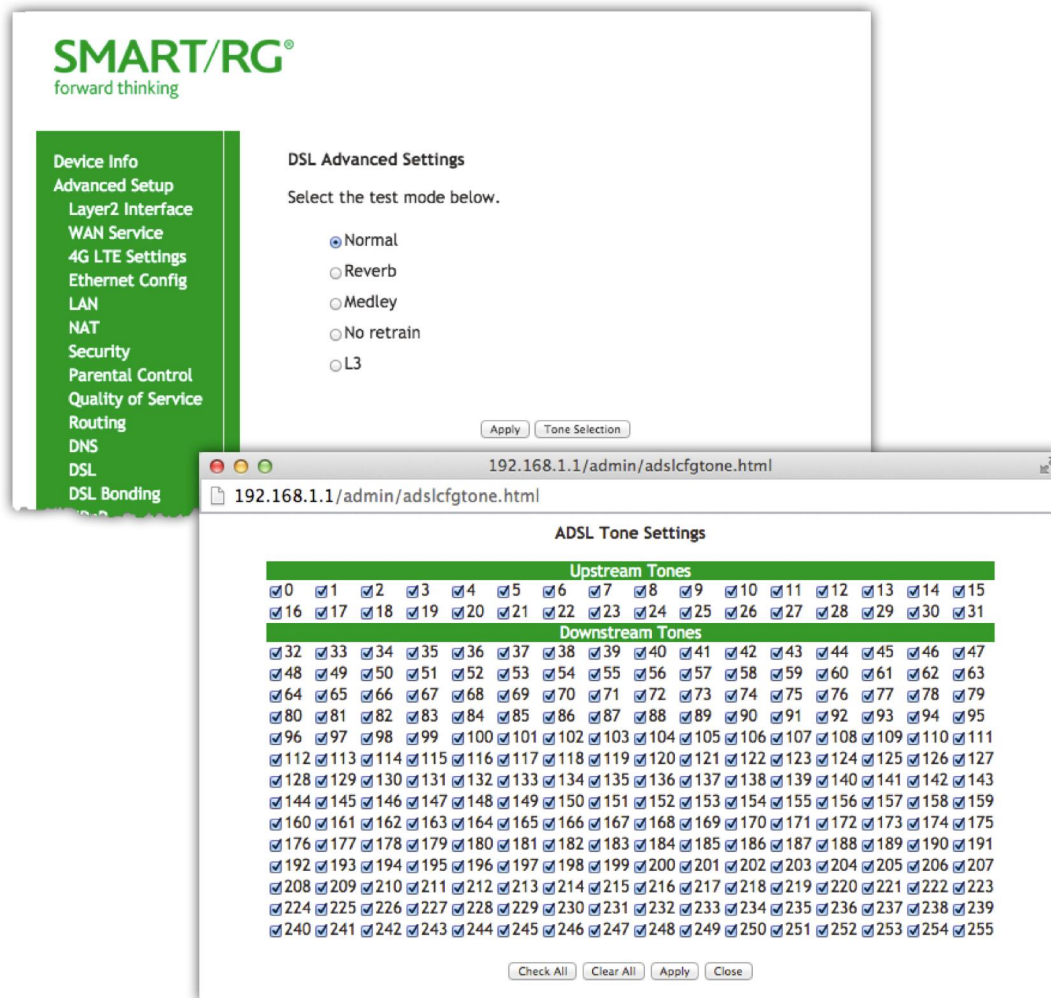
Modulation	Data Transmission Rate
AnnexL	Annex L of ITU-T G.992.3 standard which supports longer loops but with reduced transmission rates.
ADSL2+	ITU-T G.992.5 standard. Max Downstream: 28 Mbps Max Upstream: 1.0 Mbps
AnnexM	Annex L of ITU-T G.992.5 standard which supports extended upstream bandwidth. Max Downstream: 24 Mbps Max Upstream: 3 Mbps
VDSL2	ITU-T G.993.2 standard. Max Downstream: 100 Mbps Max Upstream: 60 Mbps

Parameter	8a	8b	8c	8d	12a	12b	17a
Max DS Tx Power (dBm)	+17.5	+20.5	+11.5		+14.5		
Max US Tx Power (dBm)				+14.5			
Min bidirectional net data rate		50Mbps			68Mbps	100Mbps	

Other Settings	
Field Name	Description
Inner Pair/Outer Pair	The RJ11 connector has four contacts. The center pair of pins is DSL1. The outer pair pins are the contacts for DSL2. Select which pair should be used.
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation

Test Modes	
Mode	Description
Normal	Puts the DSL PHY in test mode, sending only a Normal signal.
Reverb	Puts the DSL PHY in test mode, sending only a REVERB signal
Medley	Puts the DSL PHY in test mode, sending only a MEDLEY signal.
No Retrain	The DSL PHY will attempt to establish a connection as in Normal mode, but once the connection is up, it will not retrain even if the signal is lost.
L3	Puts the DSL modem in the L3 power state.

Click the [Apply](#) button to place the gateway in test mode.



CAUTION: Do not modify the tones selected unless under explicit instruction from a telecommunications professional.

Click the **Apply** button to commit your changes.

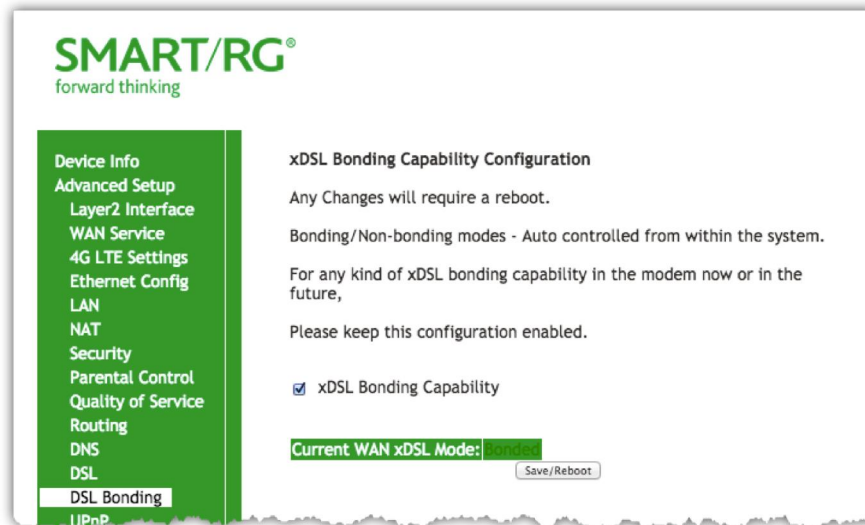
DSL Bonding

NOTE: This feature supported only on SmartRG models SR550n and SR552n.

Bonding enables two DSL lines to feed the same modem. Utilize this screen to leverage the bandwidth of both lines. Bonded, they will behave as a single, higher bandwidth connection.

After selecting **Advanced Setup -> DSL Bonding** from the left navigation bar. The following screen will appear. Check the checkbox to enable Bonding.

Click [Save/Reboot](#) to commit your changes.

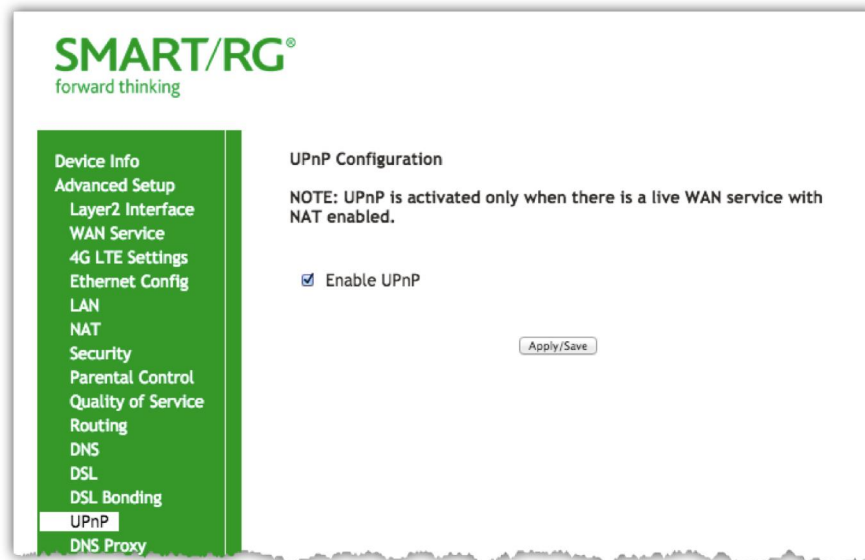


UPnP

Enable UPnP when 3rd party devices on your LAN support this Universal Plug and Play standard. Common client devices include gaming consoles, IP cameras, printers and others.

After selecting [Advanced Setup](#) -> [UPnP](#) from the left navigation bar. The following screen will appear. Check the checkbox to enable UPnP.

Click [Apply/Save](#) to commit your changes.

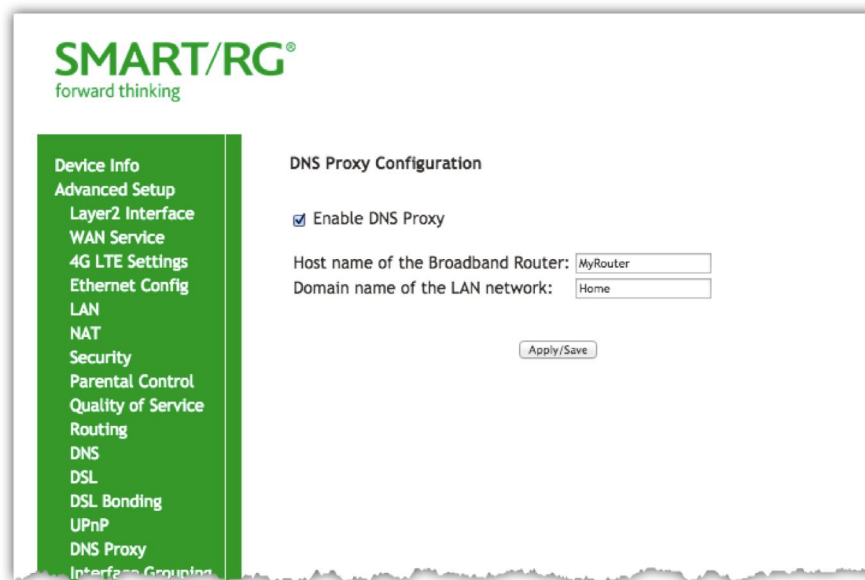


DNS Proxy

A DNS Proxy improves domain look-up performance for clients by creating a historical cache of look-ups. Navigate to [Advanced Setup](#) -> [DNS Proxy](#) to enable and configure this feature.

After selecting [Advanced Setup](#) -> [DNS Proxy](#) from the left navigation bar. The following screen will appear. Check the check-box to enable DNS Proxy mode and specify a Host-name and Domain Name of the LAN in the fields that follow.

Click [Apply/Save](#) to commit your changes.



Interface Grouping

Creating an interface group is used to map local interfaces to WAN interfaces. Typical application for this feature would include assigning IPTV STBs to a WAN interface.

After selecting **Advanced Setup** -> **Interface Grouping** from the left navigation bar, click the **Add** button below the table. The screen shown on the next page will appear.

To create a new interface group:

1. Enter a unique **Group Name** then select either step 2. (dynamic) or step 3. (static) below:
2. To automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP vendor ID string, any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select an interface from the **Available Interface** list and add it to the **Grouped Interface** list using the arrow buttons to create the required mapping of the ports. Hold down the shift key to multi-select. NOTE: These clients may obtain public IP addresses.
4. If this interface is to share the WAN interface, click the **Shared WAN Interface** box. Not checking this will cause the WAN interface you select to be removed from any other interface groups.

SMART/RG®
forward thinking

- Device Info
- Advanced Setup
 - Layer2 Interface
 - WAN Service
 - 4G LTE Settings
 - Ethernet Config
 - LAN
 - NAT
 - Security
 - Parental Control
 - Quality of Service
 - Routing
 - DNS
 - DSL
 - DSL Bonding
 - UPnP
 - DNS Proxy
 - Interface Grouping**
 - IP Tunnel
 - IPSec
 - Certificate
 - Multicast
- Wireless
- Diagnostics
- Management
- Logout

Group Name:

Shared WAN Interface: ☐

Grouped WAN Interfaces

Available WAN Interfaces

br_0_0_1/ptm0
No Interface/None

Grouped LAN Interfaces

Available LAN Interfaces

LAN4
LAN3
LAN2
LAN1
WAN

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

Click [Apply/Save](#) to commit. Your changes will be effective immediately.

IP Tunnel

IP Tunneling is typically used as a means to establish a path between two independent networks. Your SmartRG gateway supports connecting islands of IPv6 networks across the IPv4 internet or IPv4 in IPv6 as well.

IPv6inIPv4

After selecting [Advanced Setup](#) -> [IP Tunnel](#) -> [IPv6inIPv4](#) from the left navigation bar, click the Add button. The screen shown on the next page will appear.

1. Enter a **Tunnel Name**
2. Currently, only the 6rd **Mechanism** is supported
3. Select the appropriate LAN and WAN interfaces from the drop-down lists associated with the tunnel you wish to establish.
4. **IPv4 Mask Length**, **6rd Prefix with Prefix Length** and **Border Relay IPv4 Address** can be configured automatically. Select the **Manual** radio button to specify your desired settings for these fields.

Click **Apply/Save** to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPv6inIPv4
IPv4inIPv6
IPSec

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

☒ Manual ☐ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

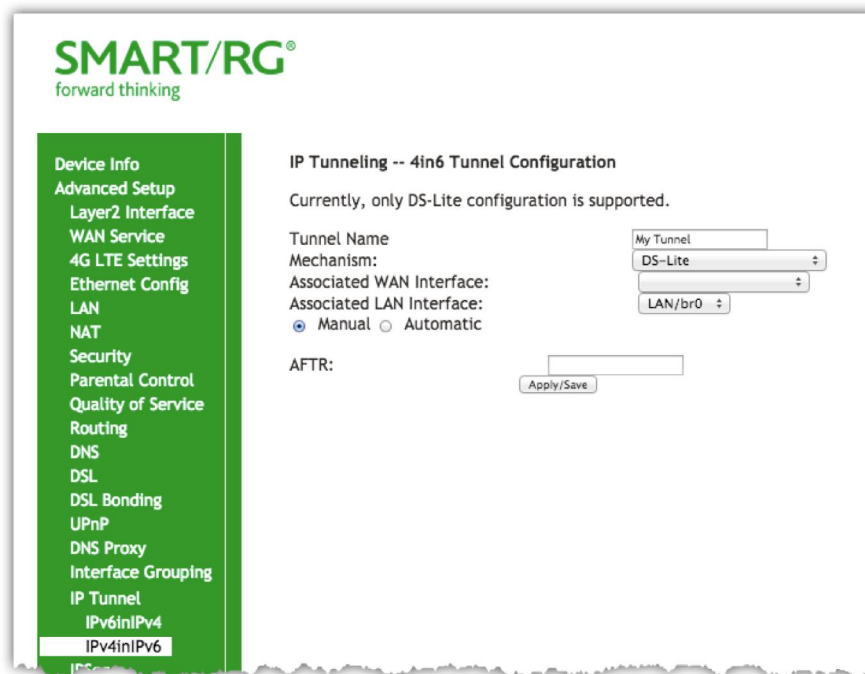
Border Relay IPv4 Address:

IPv4inIPv6

After selecting **Advanced Setup -> IP Tunnel -> IPv4inIPv6** from the left navigation bar, click the **Add** button. The screen shown on the next page will appear.

1. Enter a **Tunnel Name**
2. Currently, only the DS-Lite **Mechanism** is supported. Consult RFC6333 for further information regarding DS-Lite.
3. Select the appropriate **LAN** and **WAN** interfaces from the drop-down lists associated with the tunnel you wish to establish.
4. AFTR (Address Family Transition Router) may be configured automatically. Select the **Manual** radio button to specify your desired value for fields.

Click **Apply/Save** to commit your changes.



IPSec

Internet Protocol Security is a protocol for securing communications by packet level encryption and authentication. Use the IPSec page to enable and remove connections, or edit existing connections. The **IPSec** configuration screen is dynamic. Some options are revealed or hidden depending on the selected connection.

After selecting **Advanced Setup -> IP Sec** from the left navigation bar, click the **Add New Connection**. The following screen will appear. Enter your connection details by completing the appropriate fields.

Click **Apply/Save** to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPv6inIPv4
IPv4inIPv6
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

IPSec Settings

IPSec Connection Name

IP Version:

Tunnel Mode

Local Gateway Interface:

Remote IPsec Gateway Address

Tunnel access from local IP addresses

IP Address for VPN

Mask or Prefix Length

Tunnel access from remote IP addresses

IP Address for VPN

Mask or Prefix Length

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

The individual fields on this screen are defined as follows:

Field Name	Description
IPSec Connection Name	A free form text field. Enter a descriptive name for this connection
IP Version	[IPv4, IPv6] Select the IP version environment associated with your infrastructure.
Tunnel Mode	[ESP, AH] Select encapsulation method to be used. Use AH tunnel mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed. Use ESP tunnel mode to encapsulate a packet with ESP and IP headers. An ESP trailer is added to the packet for authentication and integrity.
Local Gateway Interface	Select the WAN connection from the drop-down list to be associated with this tunnel.
Remote IPsec Gateway Address	Enter the WAN IP for tunnel.

Field Name	Description
Tunnel Access From Local IP Addresses	[Subnet, Single Address] Select IP information for site A and B. Subnet indicates entire LAN. For single host, select Single Address.
Key Exchange Method	[Manual, Auto (IKE)] The default of Auto (IKE) which uses the negotiated key-exchange method for IPSec is recommended.
Authentication Method	[Pre-Shared Key, Certificate (x.509)] Select the method by which the remote end will authenticate.
Perfect forwarding Secrecy	[Enable, Disable] When enabled, this setting ensures that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future.

If desired, use the [Advanced IKE Settings](#) area to select Phase 1 and Phase 2 specific parameters.

Certificate

Use the [Advanced Setup -> Certificate](#) pages to configure certificates for the gateway. Certificates contain public keys as well as the identity of the owner. They verify a person's identity. You can use Local and Trusted CA certificates on this gateway.

Local

Use the [Local](#) Certificate page to configure certificates for the gateway. Local certificates are used to identify the gateway to other users. You can create a new certificate request locally and have it signed by a certificate authority or import an existing certificate. Consult ITU-T X.509 for additional info regarding Public Key Infrastructure (PKI).

After selecting [Advanced Setup -> Certificate -> Local](#) from the left navigation bar, click the [Create Certificate Request](#) button. This function facilitates the application process for a new certificate. Complete the necessary fields.

The screen shown on the next page will appear. Enter your connection details by completing the appropriate fields.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Local
Trusted CA
Multicast

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:
 Common Name:
 Organization Name:
 State/Province Name:
 Country/Region Name:

The individual fields on this screen are defined as follows:

Field Name	Description
Certificate Name	A free form text field. Typically used to describe the intended use of the certificate.
Common Name	Enter the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes and is a free-form text field.
Organization Name	A free form text field. Typically the company name creating the request.
Country/Region	Select the Country/Region in which this certificate will be employed.

Click **Apply** to complete the request.

Reference the [ITU X.509](#) standard for certificate related details.

The **Import Certificate** button on the **Local** landing page facilitates putting the signed Certificate and corresponding Private Key information into place.

1. Enter "cpecert" for this field.
2. Paste the **Certificate** details as indicated between the **BEGIN** and **END** markers.
3. Paste the **Private Key** information as indicated between the **BEGIN** and **END** markers.

Click **Apply** to commit this Certificate.

Trusted CA

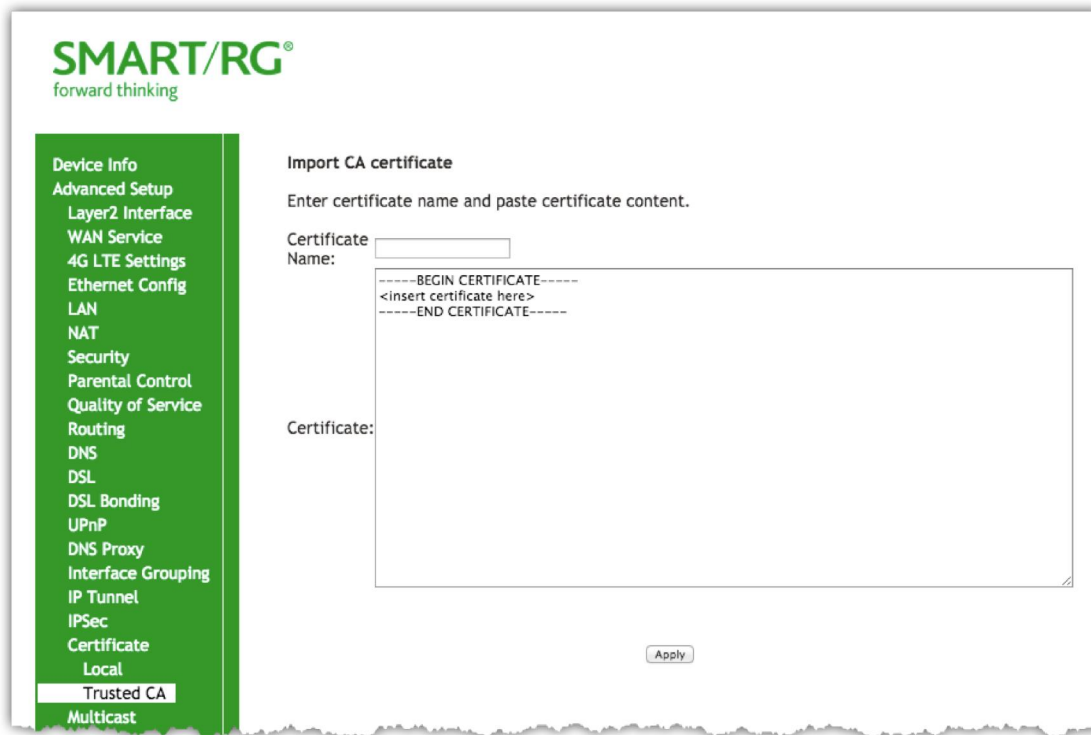
Use Trusted Certificates to identify other gateways to your gateway as a trusted source. You can import and store four trusted certificates on the gateway. Store up to four peer certificates using this feature.

After selecting **Advanced Setup -> Certificate -> Trusted CA** from the left navigation bar, click the **Import Certificate** button. The following screen will appear.

Enter "acscert" for the **Certificate Name** field then paste the Certificate details as indicated between the **BEGIN** and **END** markers.

Click **Apply** to commit this Certificate.

After adding one certificate, a **Remove** button will be revealed on the **Trusted CA** landing page.



Multicast

Multicast is the methodology for applications shipping information simultaneously to multiple destinations. The most common scenario being Internet television and other streaming media. In IP Multicast the implementation occurs at the IP routing level, where routers create the most efficient distribution paths for packets sent to a destination.

Select **Advanced Setup** -> **Multicast** from the left navigation bar. The screen pictured below will appear. Update or complete the necessary fields.

Click **Apply** to commit your changes.

SMART/RG®

forward thinking

Device Info
Advanced Setup
Layer2 Interface
WAN Service
4G LTE Settings
Ethernet Config
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Interface Grouping
IP Tunnel
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management
Logout

Multicast Precedence: Disable lower value, higher priority

IGMP Configuration
Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version: 3
Query Interval: 125
Query Response Interval: 10
Last Member Query Interval: 10
Robustness Value: 2
Maximum Multicast Groups: 25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24): 10
Maximum Multicast Group Members: 25
Fast Leave Enable: ☒
LAN to LAN (Intra LAN) Multicast Enable: ☐
Membership Join Immediate (IPTV): ☐

MLD Configuration
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version: 2
Query Interval: 125
Query Response Interval: 10
Last Member Query Interval: 10
Robustness Value: 2
Maximum Multicast Groups: 10
Maximum Multicast Data Sources (for mldv3): 10
Maximum Multicast Group Members: 10
Fast Leave Enable: ☒
LAN to LAN (Intra LAN) Multicast Enable: ☐

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Multicast Precedence	[Enable, Disable] When enabled, the lower the multicast, the IGMP packets will be put higher in the queue.
Default Version	[1-3] Enter the supported IGMP version.
Query Interval	The interval at which the multicast router sends a query messages to hosts. Expressed in seconds. If the number is below 128, the value is used directly. If the value is greater than 128, it is interpreted as an exponent and mantissa.
Query Response Interval	Upon receiving a query packet, a host beings counting down seconds, from a random number. When the timer expires, the host sends it's report. Enter a value for the maximum number of seconds for the range of random values a host can pick to count down from. The value must be greater than the Query Interval. If using IGMP v1, this value is fixed at 10 seconds.

Field Name	Description
Last Member Query Interval	Enter the maximum response time within which the host must respond to the Out of Sequence query from the router. (Default = 1000ms) IGMP uses this value when router receives and IGMPv2 Leave report indicating at least one host wants to leave the group. Upon receiving the Leave report, the router confirms the interface is not configured for IGMP Immediate Leave. If not, the router sends the out-of-sequence query.
Robustness Value	[2-7] Enter the value representing the complexity of the query. The greater the value, the more robust the query.
Maximum Multicast Groups	Maxim number of groups allowed.
Maximum Multicast Data Sources (for IGMP v3)	[1-24] Maximum data sources allowed.
Maximum Multicast Group Members	The maximum number of multicast groups that can be joined on a port or group of ports.
Fast leave	[Enabled, Disabled] If enabled, the IGMP proxy removes group member immediately without sending a query.
LAN to LAN (Intra LAN) Multicast	Check this option to permit a multicast data source on the LAN side and IGMP snooping enabled.
Membership Join Immediate (IPTV)	When enabled, clients do not send a join report and will have faster join at startup but only by a few milliseconds.

Wireless

Basic

This page allows you to configure basic features of the Wi-Fi LAN interface. You can enable or disable the Wi-Fi LAN interface, hide the network from active scans, set the Wi-Fi network name (also known as SSID) and restrict the channel set based on country requirements.

After selecting [Wireless -> Basic](#) from the left navigation bar you may modify settings as desired.

Click [Apply/Save](#) to commit your settings.

SMART/RG®

forward thinking

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Logout

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable WiFi Button

☒ Enable Wireless

☐ Enable Wireless Hotspot2.0 [WPA2 is required!]

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☐ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Enable HSPOT	Max Clients	BSSID
☐	Guest	☐	☐	☒	☐	☐ [wpa2!]	128	N/A
☐	Guest1	☐	☐	☒	☐	☐ [wpa2!]	128	N/A
☐	Guest2	☐	☐	☒	☐	☐ [wpa2!]	128	N/A

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Enable Wireless	Check to enable the gateway's Wi-Fi radio.
Enable Wireless Hotspot2.0	Check to enable wireless Hotspot2.0. (WPA2 is required!) Hotspot 2.0 is focused on enabling a mobile device to automatically discover Wi-Fi access points that have a roaming arrangement with the user's home network and then securely connect.
Hide Access Point	Check to Hide Access Point SSID.
Client Isolation	Check to prevent LAN client devices from communicating with one another on the wireless network.

Field Name	Description
Disable WMM Advertise	Check to stop the wireless from advertising Wireless Multimedia (WMM) functionality. WMM provides basic Quality of Service (QOS) for applications.
Enable Wireless Multicast Forwarding	Check to enable Wireless Multicast Forwarding (WMF). Forwards multicast traffic across wireless clients when enabled.
SSID	Enter the the Wi-Fi Service Set Identifier (SSID) here.
BSSID	Enter the Basic Service Set Identifier (BSSID). Provides the MAC address assigned to the wireless router.
Country	Set the country in which the gateway is deployed.
Max Clients	[1-16] Define the maximum number of clients that can access the router wirelessly.
If desired, up to three virtual access points for guest use may be defined.	
Enabled	Check to Enable a virtual wireless access point for guest access.
SSID	Enter your desired wireless Service Set Identifier (SSID) here.
Hidden	Check this option to hide the SSID from being broadcasted publicly.
Isolate Clients	Check to prevent client PCâ€™s from communicating with one another.
Disable WMM Advertise	Check to stop the wireless from advertising Wireless Multimedia (WMM) functionality.
Enable WMF	Check to enable Wireless Multicast Forwarding (WMF).
Enable HSPOT	Check to enable wireless Hotspot2.0
BSSID	N/A

Security

Utilize this screen to configure security features of the wireless LAN interface.

You may configuration it manually or via Wi-Fi Protected Setup (WPS).

After selecting **Wireless -> Security** from the left navigation bar you may modify settings as desired.

Click **Apply/Save** to commit your settings.

NOTE: When both **STA PIN** and **Authorized MAC** are empty, **PBC** becomes the default value.

If **Hide Access Point** is enabled or the MAC filter list is empty with "allow" chosen, WPS2 will be disabled.

SMART/RG®
forward thinking

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS)
 Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS Enabled ▾

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)
☐ Enter STA PIN ☐ Use AP PIN Add Enrollee

Set WPS AP Mode Configured ▾

Setup AP (Configure all security settings with an external registrar)

Device PIN 76229909 [Help](#)

The individual fields on this screen are defined as follows:

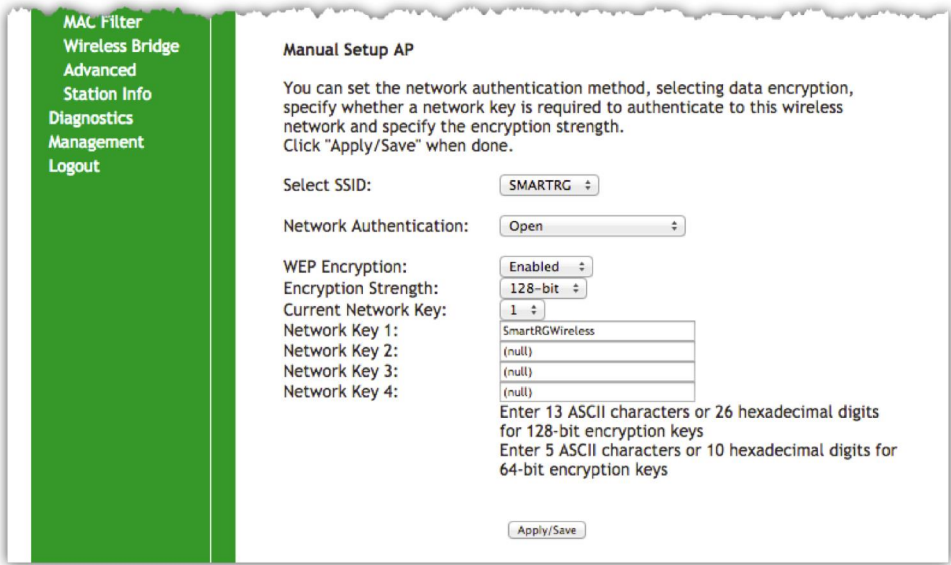
Field Name	Description
Enable WPS	[Enabled, Disabled] Enables Wi-Fi Protected Setup.
Enter STA PIN Use AP PIN	Select the method [STA PIN, AP PIN] for how the WPS PIN is generated. Select the desired radio button then click the Add Enrollee button if necessary to add a specific, enrollee station. If both the PIN field and Set Authorized Station MAC are left blank, the PBC (push-button) mode is automatically made active.
Set Authorized Station MAC	When manually pairing via WPS, enter the MAC address of the client device you are trying to connect.
Set WPS AP Mode	[Configured, Unconfigured] Select Configured to have the gateway assign security settings to clients. Select Unconfigured when you wish to have an external client assign security settings to your SmartRG gateway.
Device PIN	(Auto generated by the access point.)
Network Authentication	Select the desired network security authentication type.

Note that many of the fields in the Manual Setup portion of the screen vary based on the choice of Network Authentication. Each variation is presented below.



Manual Setup - Network Authentication: Open and Shared

The same configuration fields apply for **Manual Setup** of both **Shared** and **Open** authentication types. WPS however may not be used under **Shared**.



The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup - Network Authentication: 802.1X

Advanced Setup

Wireless

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Station Info

Diagnostics

Management

Logout

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

SMARTRG

Network Authentication:

802.1X

RADIUS Server IP Address:

0.0.0.0

RADIUS Port:

1812

RADIUS Key:

WEP Encryption:

Enabled

Encryption Strength:

128-bit

Current Network Key:

2

Network Key 1:

SmartRGWireless

Network Key 2:

(null)

Network Key 3:

(null)

Network Key 4:

(null)

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
RADIUS Server IP address	Enter the IP address for the Remote Authentication Dial In User Service server associated with your infrastructure.
RADIUS Port	Port 1812 for authentication is a standard for RADIUS authentication per the IETF RFC 2865. Your RADIUS deployment may differ from this. Older servers may use port 1645.
RADIUS Key	(Optional) Enter the encryption key (if required) to authenticate to the RADIUS Server specified via the Server IP address above.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup - Network Authentication: WPA

WPA Authentication requires the same set of parameters as used with 802.1X (above) with but with the two parameters added: **WPA Group Rekey Interval** and **WEP Encryption**. Reference the above table for field descriptions not found in the table for WPA below.

Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Logout

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: SMARTRG

Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP+AES

WEP Encryption: Disabled

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.

Manual Setup - Network Authentication: WPA-PSK

Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Logout

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: SMARTRG

Network Authentication: WPA2 -PSK

WPA passphrase: [Click here to display](#)

☐ Use base MAC address as WPA passphrase

WPA Group Rekey Interval: 0

WPA Encryption: AES

WEP Encryption: Disabled

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WPA/WAPI passphrase	Enter the desired security password to be used by this security configuration.
Use base MAC address as WAP/WAPI Passphrase	In lieu of manually entering a password, allow the Base MAC address to be substituted for the password. When this box is checked, any content in the WPA/WAPI passphrase field will be ignored.
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup - Network Authentication: WPA2

The screenshot shows the 'Manual Setup AP' configuration page. On the left is a green sidebar with navigation links: Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, Management, and Logout. The main content area is titled 'Manual Setup AP' and contains the following fields and options:

- Select SSID:** A dropdown menu showing 'SMARTRG'.
- Network Authentication:** A dropdown menu showing 'WPA2'.
- WPA2 Preauthentication:** A dropdown menu showing 'Disabled'.
- Network Re-auth Interval:** A text input field with the value '36000'.
- WPA Group Rekey Interval:** A text input field with the value '0'.
- RADIUS Server IP Address:** A text input field with the value '0.0.0.0'.
- RADIUS Port:** A text input field with the value '1812'.
- RADIUS Key:** A text input field.
- WPA Encryption:** A dropdown menu showing 'AES'.
- WEP Encryption:** A dropdown menu showing 'Disabled'.
- Apply/Save:** A button at the bottom right.

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WPA2 Preauthentication	
Network Re-Auth Interval	
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
RADIUS Server IP address	Enter the IP address for the Remote Authentication Dial In User Service server associated with your infrastructure.
RADIUS Port	[1-65535] Port 1812 for authentication is a standard for RADIUS authentication per the IETF RFC 2865. Your RADIUS deployment may differ from this. Older servers may use port 1645.
RADIUS Key	Enter the encryption key required to authenticate to the Radius Server specified via the Server IP address above.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup - Network Authentication: WPA2-PSK

The screenshot shows the 'Manual Setup AP' page in the SMART/RG web interface. On the left is a green sidebar with navigation links: Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, Management, and Logout. The main content area is titled 'Manual Setup AP' and contains the following fields and options:

- Select SSID:** A dropdown menu showing 'SMARTRG'.
- Network Authentication:** A dropdown menu showing 'WPA-PSK'.
- WPA passphrase:** A text field with masked characters (dots) and a link 'Click here to display'.
- ☐ Use base MAC address as WPA passphrase
- WPA Group Rekey Interval:** A text field with the value '0'.
- WPA Encryption:** A dropdown menu showing 'TKIP+AES'.
- WEP Encryption:** A dropdown menu showing 'Disabled'.
- Apply/Save:** A button at the bottom right.

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WPA/WAPI passphrase	Enter the desired security password to be used by this security configuration.
Use base MAC address as WAP/WAPI Passphrase	In lieu of manually entering a password, allow the Base MAC address to be substituted for the password. When this box is checked, any content in the WPA/WAPI passphrase field will be ignored.
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup - Network Authentication: Mixed WPA2-WPA

The screenshot shows the 'Manual Setup AP' configuration page. On the left is a green sidebar menu with options: Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, Management, and Logout. The main content area is titled 'Manual Setup AP' and contains the following fields:

- Select SSID: SMARTRG (dropdown)
- Network Authentication: Mixed WPA2/WPA (dropdown)
- WPA2 Preauthentication: Disabled (dropdown)
- Network Re-auth Interval: 36000 (text input)
- WPA Group Rekey Interval: 0 (text input)
- RADIUS Server IP Address: 0.0.0.0 (text input)
- RADIUS Port: 1812 (text input)
- RADIUS Key: (text input)
- WPA Encryption: TKIP+AES (dropdown)
- WEP Encryption: Disabled (dropdown)
- Apply/Save button

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WPA2 Preauthentication	

Field Name	Description
Network Re-Auth Interval	
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
RADIUS Server IP address	Enter the IP address for the Remote Authentication Dial In User Service server associated with your infrastructure.
RADIUS Port	Port 1812 for authentication is a standard for RADIUS authentication per the IETF RFC 2865. Your RADIUS deployment may differ from this. Older servers may use port 1645.
RADIUS Key	Enter the encryption key required to authenticate to the Radius Server specified via the Server IP address above.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

Manual Setup

Network Authentication: Mixed WPA2/WPA-PSK

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: SMARTRG

Network Authentication: Mixed WPA2/WPA-PSK

WPA passphrase: [Click here to display](#)

☐ Use base MAC address as WPA passphrase

WPA Group Rekey Interval: 0

WPA Encryption: TKIP+AES

WEP Encryption: Disabled

Apply/Save

The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID from the drop-down list for the wireless network to which this security configuration will apply.
WPA2 Preauthentication	When enabled, clients can pre-authenticate with the gateway while still connected to another AP.
Network Re-Auth Interval	[0-2,147,483,647 seconds] The interval that the client must re-authenticate with the gateway.
WPA Group Rekey Interval	[1-65535 seconds] The frequency with which the gateway automatically updates the group key and sends it to connected LAN client devices.
WPA/WAPI Encryption	[AES, TKIP+AES] Choose from Advanced Encryption Standard (AES) or AES combined with Temporary Key Integrity Protocol (TKIP). This field has been pre-populated with the option most complimentary to the Network Authentication selected.
WEP Encryption	[Enabled, Disabled] Select Enabled to turn on Wired Equivalent Privacy mode.
Encryption Strength	[128 bit, 64 bit] Select the length of the encryption method. 128 bit being the more robust option for security.
Current Network Key	[1-4] Select which of the four keys from the list is presently in effect.
Network Key 1-4	Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128 or 64 bit).

MAC Filter

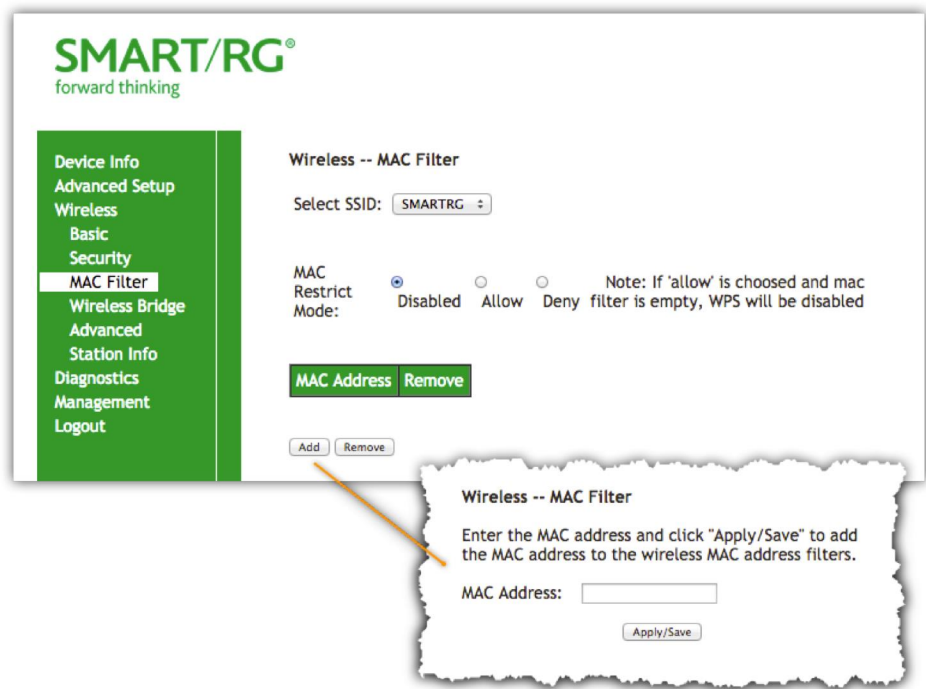
Also known as Layer 2 address filtering, MAC Filtering refers to an access control methodology whereby the 48-bit address assigned to each LAN host NIC is used to determine access to the network.

After selecting **Wireless -> MAC Filter** from the left navigation bar, select an SSID to filter from the drop-down list.

Next, select the **MAC Restrict Mode** (Disabled, Allow or Deny).

Use the **Add** button to add a MAC address to the filter list.

Click **Apply/Save** to commit the completed entry.



The individual fields on this screen are defined as follows:

Field Name	Description
Select SSID	Select the SSID to apply this MAC filter rule to.
MAC Restrict Mode	Disabled: MAC filtering is off.
	Allow: For specified MAC address, access is permitted.
	Deny: Access for the specified MAC address is rejected.

Wireless Bridge

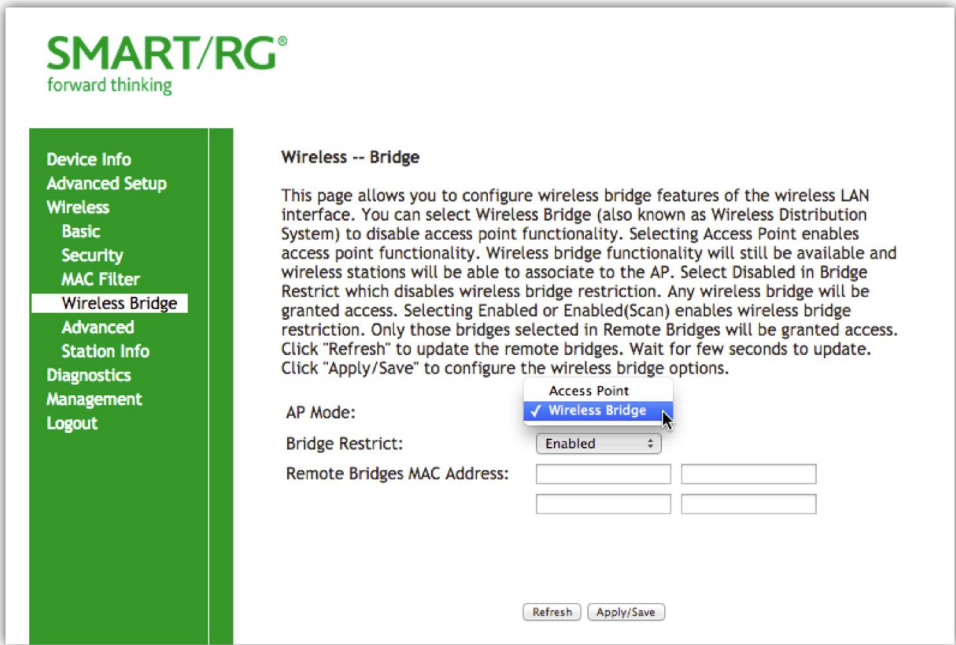
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select **Wireless Bridge** (also known as Wireless Distribution System) to disable access point functionality. Selecting **Access Point** enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the Access Point.

Selecting **Disabled** in Bridge Restrict will disable wireless bridge restriction. Any wireless bridge will be granted access. Selecting **Enabled** or **Enabled(Scan)** enables wireless bridge restriction. Only those bridges specified via their MAC address in Remote Bridges will be granted access.

After selecting **Wireless -> Wireless Bridge** from the left navigation bar, enter your settings as desired.

Click **Refresh** to update the remote bridges. Wait for few seconds to update.

Click **Apply/Save** to commit your changes.



The individual fields on this screen are defined as follows:

Field Name	Description
AP Mode	[Wireless Bridge, Access Point] Select Wireless Bridge to disable Access Point functionality. Select Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	[Enabled, Disabled] Optional setting to turn off wireless bridge restriction. When disabled, any wireless bridge will be granted access. Choose Enabled or Enabled (Scan) to turn on wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Use the Refresh button to update the station list when Bridge Restrict is enabled.
Remote Bridge MAC Address	Enter the MAC address(es) of the remote bridges to be allowed

Advanced

At **Wireless -> Advanced** you may configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a desired speed, set the fragmentation threshold, the RTS threshold, the wakeup interval for clients in power-save mode, and more.

After selecting **Wireless -> Advanced** from the left navigation bar, enter your settings as desired.

Click **Apply/Save** to commit your changes.

SMART/RG®
forward thinking

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Logout

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band: 2.4GHz
Channel: Auto
Auto Channel Timer(min): 5
802.11n/EWC: Auto
Bandwidth: 20MHz
Control Sideband: Lower
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
RIFS Advertisement: Auto
OBSS Coexistence: Enable
RX Chain Power Save: Disable
RX Chain Power Save Quiet Time: 10
RX Chain Power Save PPS: 10
54g™ Rate: 1 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 128
XPress™ Technology: Enabled
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled
WMM No Acknowledgement: Disabled
WMM APSD: Enabled

Current: 1 (interference: acceptable)

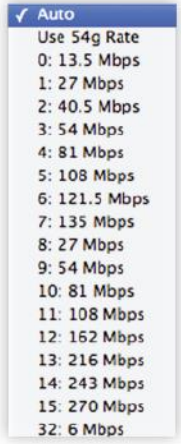
Current: 20MHz
Current: N/A

Power Save status: Full Power

Apply/Save

The individual fields on this screen are defined as follows:

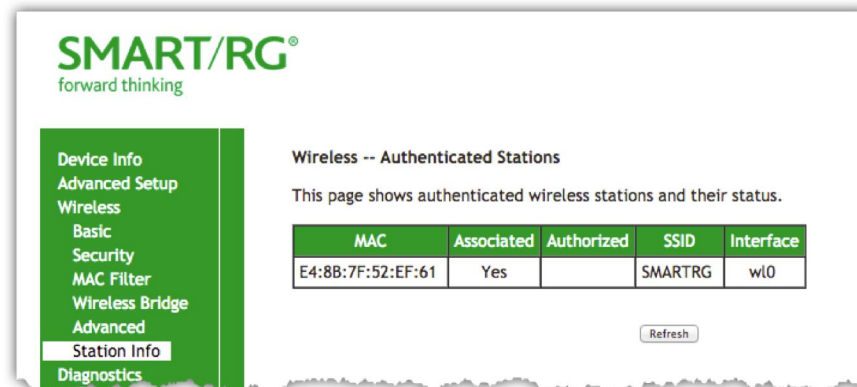
Field Name	Description
Band	Pre-set at 2.4 GHz for compatibility with IEEE 802.11x standards.
Channel	[Auto, 1-11] Select the Wi-Fi channel you wish to use.
Auto Channel Timer(min)	[0-65535 minutes] Set the frequency with which the gateway scans channels for interference. If a threshold of inference is detected, a new channel will be auto selected.
802.11n/EWC	[Auto, Disabled] Reference, IEEE 802.11n Draft 2.0 for details on this standard.
Bandwidth	[20MHz, 40MHz] Select the Bandwidth. 40MHz bandwidth provides better throughput by taking advantage of two, adjacent 20MHz bands.
Control Sideband	[Upper, Lower] Select the appropriate sideband to minimize RF interference from adjacent channels and maximize the throughput. Sideband controls only available in 40MHz mode.

Field Name	Description
802.11n rate	Select the desired physical transmission rate. 
802.11n protection	[Off, Auto] Select Auto for maximum security but there is a noticeable impact on throughput. Select Off for best throughput.
Support 802.11n client only	[On, Off] Select On to restrict 802.11b/g clients from accessing the gateway.
RIFS Advertisement	[Off, Auto] Reduced Inter-Frame Space RIFS. Improves performance by reducing dead time required between OFDM transmissions. Recommended primarily for greenfield deployments only.
OBSS Coexistence	[Enable, Disable] Coexistence of Overlapping Basic Service Sets that prevents overlapping in the 20MHz and 40MHz frequencies. If set to Enable, the gateway will automatically revert to 20MHz channel bandwidth when another WiFi network within 2 channels of its own channel is detected or when a client device with its 40MHz Intolerant bit set is detected. Disabling this feature violates the 802.11-2012 specification.
RX power chain save	[Enable, Disable] Turn on power save mode. NOTE: Set 802.11n/EWC to Auto and to Enable before setting this parameter.
RX power chain save quiet time	[0 to 2147483647 seconds] Set the delay time between when system activity ceases and power save mode engages. NOTE: Set 802.11n/EWC to Auto and to Enable before setting this parameter.
RX power chain save PPS	[0 to 2147483647 packets per second] Sets a throughput threshold for when the router engages power save mode after the quiet time seconds have elapsed. NOTE: Set 802.11n/EWC to Auto and to Enable before setting this parameter.
54g rate	[Auto, 11 Mbps, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps] Select a fixed data rate from the drop-down list if desired. Auto will select 11 Mbps when possible but will drop (based on signal strength) when necessary.
Multicast rate	[1-54 Mbps] Enter the desired packet transmit rate for multicast.
Basic Rate Fragmentation Threshold	[256 - 2346 bytes] Enter the threshold for what sized packets will be fragmented to a smaller unit size. The primary consideration for this setting being the size/capability of the circuit. A high packet error rate is an indication that a slightly increased Fragmentation Threshold is in order. When possible, the default value of 2346 should be maintained. Poor throughput is a likely result of setting this threshold too low.
RTS Threshold	[256 - 2346 bytes] Specify the Request to Send packet size beyond which the WLAN client hardware invokes its RTS/CTS mechanism. Smaller packets will otherwise be sent not using RTS/CTS. The threshold is off when using the default setting of 2347.

Field Name	Description
DTIM Interval	[1 and 65535] a.k.a. Beacon rate, Delivery Traffic Indication Message is a countdown variable indicating when the next window for listening to buffered broadcast and multicast messages is available to client devices. The default is 1.
Beacon Interval	[1 and 65535 ms] The time interval between beacon transmissions. Beacon transmissions make known the presence of an access point and convey to wireless NICs when to awake from power save mode to check for buffered frames at the access point). The default is 100 ms.
Global Max Clients	[1-255] The maximum number of client devices that can connect to the router.
Xpress TM Technology	[Enabled, Disabled] Xpress Technology is compliant with draft specifications of two planned wireless industry standards
Transmit Power	Set the desired output power (by percentage).
WMM (Wi-Fi Multimedia)	[Auto, Enabled, Disabled] When enable, this technology allows multimedia services (audio, video and voice packets) to get higher priority.
WMM Acknowledgement	No [Enabled, Disabled] Refers to the acknowledge policy used at the MAC level. Enable no Acknowledgement for better throughput but in the event of a noisy RF environment, higher error rates may result.
WMM APSD	[Enabled, Disabled] Automatic Power Save Delivery, a power consumption saving feature.

Station Info

This page displays authenticated wireless stations and their status.



Diagnostics

Line performance diagnostic tools are supported by your SmartRG gateway. Three legs of the data path are included in the available tests: LAN connectivity, DSL connectivity and Internet connectivity tests.

Diagnostics

After selecting **Diagnostics** -> **Diagnostics** from the left navigation bar, click the **Test** button at the bottom of the screen.

The table will be updated with fresh diagnostic information regarding connection integrity. There is significant in-line documentation regarding each individual test. Click the **Help** link at the far right of each line item to learn more about what is being tested and what actions to take in the event that a particular test should fail.

The normal test method is initiated with the **Test** button and utilizes OAM F5 loopback cells. Selecting the **Test With OAM F4** will conduct the test at the VP level in lieu of at an individual VC connection.

SMART/RG®
forward thinking

br_0_0_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your WAN Connection:	PASS	Help
Test your USB Connection:		Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

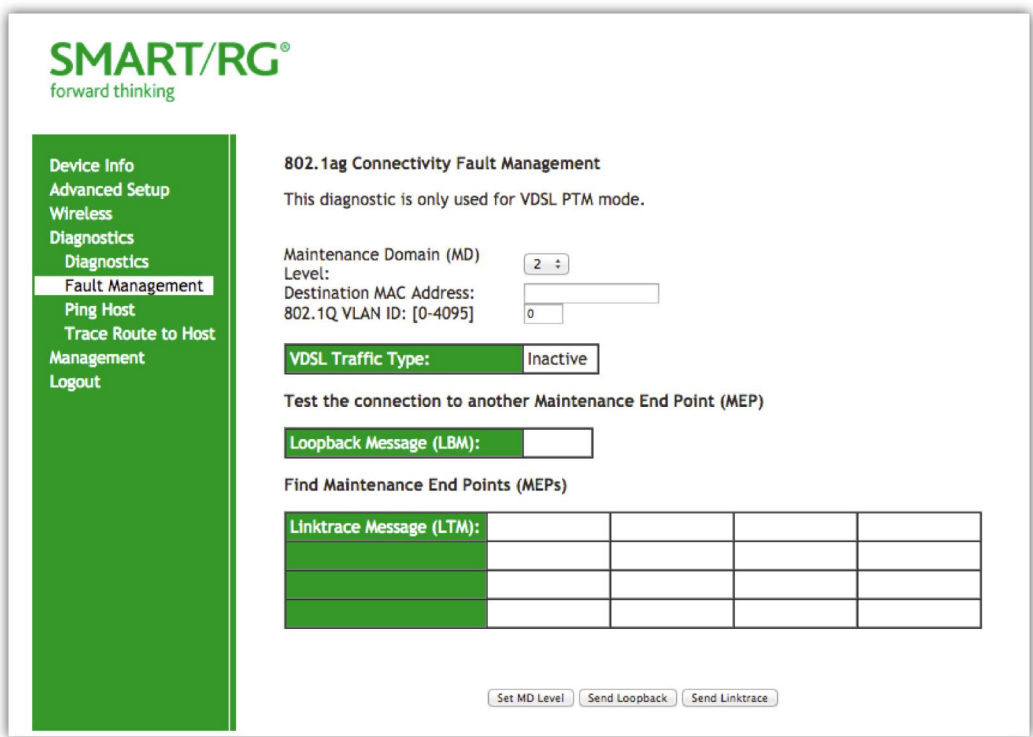
Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

[Test](#) [Test With OAM F4](#)

Fault Management

Utilize this screen for diagnostics regarding your VDSL PTM or Ethernet WAN connection. Fault Management is compliant with IEEE 802.1ag for Connectivity Fault Management.

After selecting **Diagnostics** -> **Fault Management** from the left navigation bar, select values for the **Maintenance Domain (MD) Level**, **Destination MAC Address** to test and enter the applicable (if any) **802.1Q VLAN ID**.



The individual fields on this screen are defined as follows:

Field Name	Description
Maintenance Domain (MD) Level	[0-7] Maintenance Domains are management space on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchical relationship exists between domains based on levels. The larger the domain, the higher the level value.
Looback Message (LBM)	Used on-demand as the first step to isolate a fault.
Maintenance End Point (MEP)	Points at the edge of the domain, defines the boundary for the domain.
Linktrace Message (LTM)	Identifies all maintenance points in the entity.

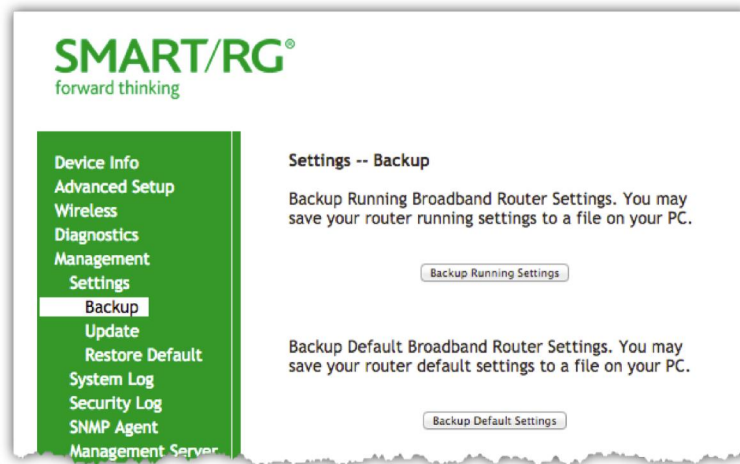
Management Settings

Backup

Current settings for your gateway can be backed up to a file stored on your computer.

After selecting **Management -> Settings -> Backup** from the left navigation bar, the following screen will appear.

Select the type of backup you desire.



The individual fields on this screen are defined as follows:

Field Name	Description
Backup Running Settings	This button will locally save a backup file of the currently running settings
Backup Default Settings	This button will locally save a backup file of the Defaulted settings

Update

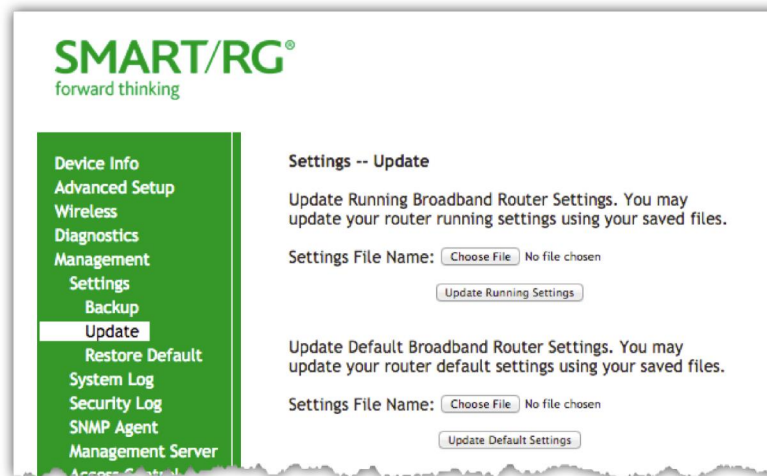
Use the features on this screen to restore previously backed-up gateway settings. Both Current and Default settings can be managed here.

After selecting **Management -> Settings -> Update** from the left navigation bar, the following screen will appear.

Click the appropriate **Choose File** button for the type of setting you wish to restore.

Next, browse to the desired .conf file located on your personal computer.

Lastly, click the **Update** button.



The individual fields on this screen are defined as follows:

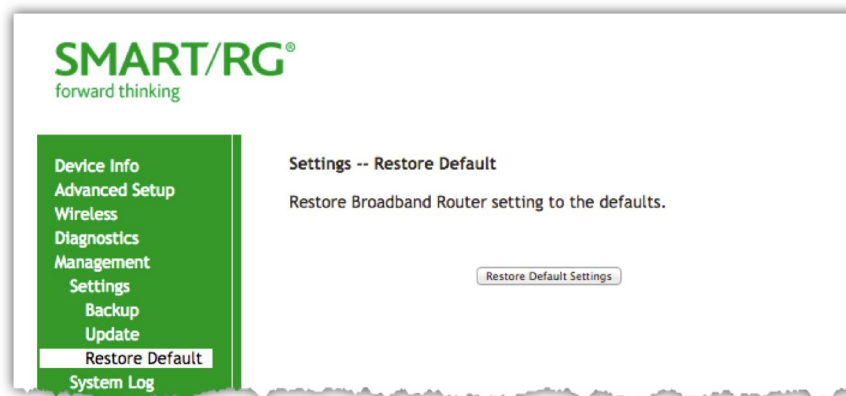
Field Name	Description
Update Running Settings	This button will allow you to select a .conf backup file to update the currently running settings
Update Default Settings	This button will allow you to select a .conf backup file to update the Defaulted settings

Restore Default

Use this screen to reset the gateway to its Default settings. Defaults can be customized and stored. For details, see Backup and Restore Settings sections of this user manual.

After selecting **Management -> Settings -> Restore Default** from the left navigation bar, the following screen will appear.

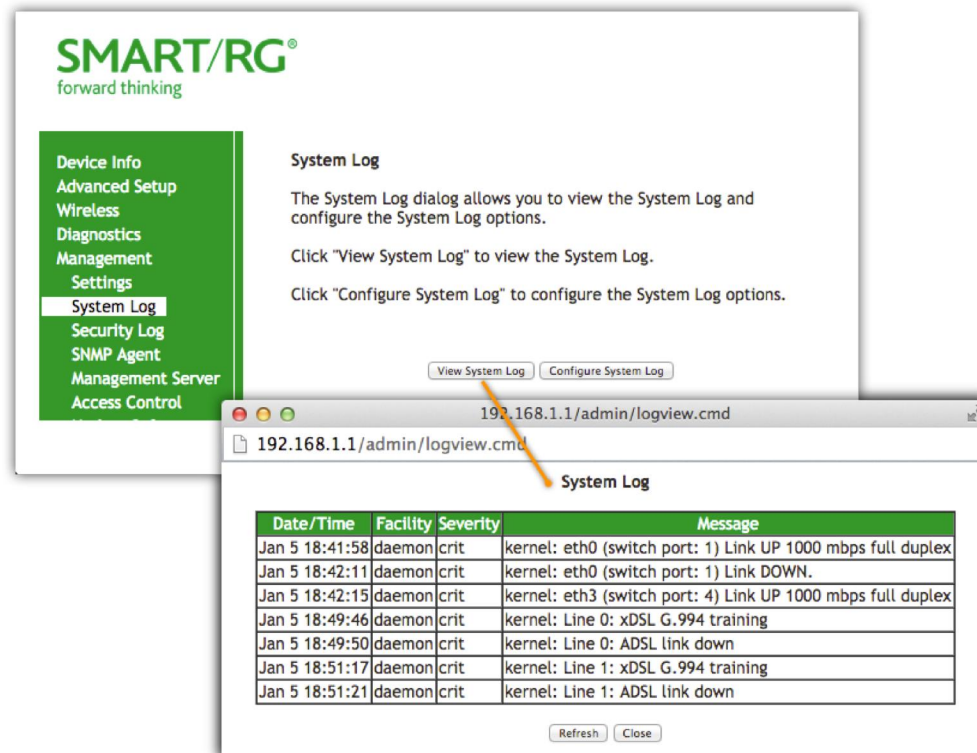
Click the **Restore Default Settings** button.



System Log

In the System Log you will find a history of error conditions and other events encountered by your gateway. Use the features on this screen to view or alter the behavior of the System Log.

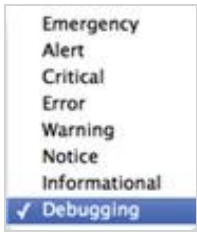
Upon selecting **Management -> Settings -> System Log** from the left navigation bar, the following screen will appear.



The individual fields on this screen are defined as follows:

Action	Description
View System Log	This button will display the system log.
Configure System Log	This button will edit the system log settings.

The following table describes the options for configuration of the System Log:

Action	Description
Enable/Disable	Select to turn logging completely off or on.
Logging Level	 Select the Error option is (least verbose) unless actively troubleshooting a situation with a subscriber for which increased log detail is required.
Display Level	Options are displayed in top-down order of least verbose to most verbose. Error option is recommended (least verbose) unless actively troubleshooting a situation with a subscriber for which increased detail is required.
Mode	Control where log events will be sent. Choose 'Remote' or 'Both' to send to the specified IP address and UDP port of a remote syslog server. Choose 'Local' or 'Both' to record events in the local memory of your SmartRG gateway.

Security Log

The security log contains a history of events related to sensitive access to the gateway. Logged events include:

- Password change success
- Password change failure
- Authorized login success
- Authorized login fail
- Authorized user logged out
- Security lockout added
- Security lockout removed
- Authorized resource access
- Unauthorized resource access
- Software update

Upon selecting **Management** -> **Settings** -> **Security Log** from the left navigation bar, the following screen will appear.



The individual fields on this screen are defined as follows:

Action	Description
View	This button will display the Security Log on the screen.
Reset	This button will purge all stored data from the Security Log.

Management Server

Management Server refers to an Auto Configuration Server such as Cisco Prime Home which offers significant advantages in terms of automation and productivity when managing subscriber devices in the field.

TR-069 Client

SmartRG gateways support TR-069 based standards for remote management. Utilize this screen to configure the gateway with details about the management ACS (Auto Configuration Server) to which this gateway will be linked.

The TR-069 client screen is preset with default connection parameters and generally only needs to be Enabled and pointed to the ACS URL. Also necessary are any required ACS Username and ACS Password. Default username and password are typically admin/admin for Connection Request defaults. Consult available ACS manufacturer's documentation if these values need to be altered.

Select **Management -> Management Server -> TR-069 Management** from the left navigation bar. The screen pictured below will appear. Update or complete the necessary fields per the instructions from your ACS platform vendor.

Click **Apply/Save** to commit your changes.

NOTE: This document does not cover the corresponding setup of your ACS. Please consult the materials provided by your ACS vendor to ensure parameters and server settings are appropriate for remote WAN side management via an ACS using the TR-069 Protocol.

SMART/RG®
forward thinking

TR-069 Client -- Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

OUI-Serial: ☒ MAC Serial Number ☐ DisableEnable

TR-069 Client: ☐ Disable ☒ Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

TR-069 Client Port:

WAN Interface used by TR-069 client:

☒ Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

The individual fields on this screen are defined as follows:

Field Name	Description
OUI-Serial	Select whether to use the base MAC address or the serial number of your gateway when connecting to the ACS. (Optional) For SmartRG gateways bearing firmware version 2.5.0.2 and above: Set the modem's TR-069 client to report Serial Number instead of MAC address to the ACS. This value may appear in an ACS user interface information display when looking at the device details of a particular gateway that has checked in. Enable this by selecting Serial Number as the alternate value using the radio button adjacent to this field. MAC (MAC address) is default for this field and the most typical scenario. For firmware versions prior to 2.5.0.2, MAC is the only available option.
TR-069 Client	Disable/Enable TR-069 client on the CPE. The TR-069 WAN Management Client can be disabled if no ACS is employed. Note however that if there is a possibility of adding an ACS to your infrastructure in the future, it is recommended to leave this option enabled. When this feature is set to off, every gateway deployed with this default must be manually/locally re-configured to enable this client if later needed.
Inform Interval	The frequency (in seconds) with which the CPE (gateway) checks in with the ACS to sync and exchange data. A typical production environment entails CPEs in the field informing to the ACS once/day or every 86,400 seconds.

Field Name	Description
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	User name by which this gateway logs in to the ACS.
ACS Password	Password to authenticate the above user name.
WAN Interface used by TR-069 client	Choose any WAN, LAN, Loop back or a configured connection to declare how this gateway will connect to the ACS.

* For example, enter. <http://customer.acs.youracsurl.com>, all in lower case.

The ACS URL may further include a port specification suffix e.g. <http://customer.acs.wanmanagementservices.com:30005> (Where :30005 is the port number.)

NOTE: This value may not need to be specified depending on the ACS platform in use. i.e. Cisco Prime Home would not require 3005 to be declared. Refer to your ACS platform documentation for details.

While 30005 is the default value for SmartRG gateways, some ACS product's Management Servers may require a different value for remote management. SmartRG products have technology to accommodate such requirements for several ACS products:

- Cisco Prime Home
- ClearVision
- Calix Consumer ACS
- and others

Minimum firmware v2.5.0.x is required. Please consult SmartRG Support when a change from the default is required.

Next, you may optionally configure the modem client Connection Request mechanism used by your ACS for communication with subscriber gateways.

NOTE: Please consult with your ACS vendor for any specific connection request requirement impacted by the following settings.

Use the GetRPCMethods buttons to force the gateway to attempt to sync with the ACS. This will assist you in verifying the TR-069 parameters entered above.

Field Name	Description
Connection Request Authentication	Check this checkbox if your ACS requires authenticated connection requests. Complete the additional credential fields that are exposed.
Connection Request Username	User name by which this gateway authenticates the ACS. Many ACS platforms utilize "admin", or "tr069", as typical default values but this may have been customized to some other value.
Connection Request Password	The password by which this gateway will authenticate to the ACS.
Connection Request URL	There is typically no need to set the Connection Request URL as it is normally established automatically based on the effective WAN IP. In some cases the port can be configured as needed. An example value for this field may look like, http://xxx.xxx.xxx.xxx:30005/ where the xxx values are specific WAN IP octet numbers. Note: The default port value is 30005. This may need to be configurable for interoperability as a function of ACS vendor, and so please consult with SmartRG if this is necessary.

STUN Config

STUN:

Stands for "Simple Traversal of UDP through NATs". STUN enables a device to find out its public IP address and the type of NAT service it is sitting behind.

STUN is most commonly used with older modems under ACS management connected via a NAT gateway. NAT accommodates a LAN side device that has been allocated a Private IP address such as a CPE device on a private network behind an ONT. In such an instance, the regular CWMP Connection Request mechanism to talk to the modem gateway cannot be used to initiate a session with that ACS.

STUN Server:

An entity that receives STUN requests and sends STUN responses. STUN servers are generally attached to the public Internet. When a STUN server is present within the infrastructure of the Service Provider, utilize this screen to configure this gateway with the connectivity specifics for that server.

After selecting **Management -> Management Server -> STUN Config**, check the STUN Server Support button to expose the required STUN settings. Complete each field in accordance with the implementation specifics of server.

Click the **Save/Apply** button to commit your changes.

The individual fields on this screen are defined as follows:

Field Name	Description
STUN Server Address	Character limit is 256 characters and represents the physical STUN server's assigned network address. An invalid address will produce an immediate on-screen error message from the SmartRG gateway. Note that an ACS server may also have STUN functionality running on the same physical box. Please consult your ACS vendor for implementation options and also TR-069 protocol documentation, if necessary.
STUN Server Port	[0-64435] Default = 3478. Set the port number associated with your STUN server infrastructure.

Field Name	Description
STUN Server User Name	The username by which the gateway accesses the STUN infrastructure. Max 256 characters in length. Special characters are valid. The value will be hidden.
STUN Server Password	The password by which the modem authenticates the above username to the STUN infrastructure. Max 256 characters in length. Special characters are valid. The value will be hidden.
STUN Server Maximum Keep Alive Period *	[0-Unlimited] Value is time in seconds. Default = -1 which specifies that there will be NO keep-alive period maximum limit.
STUN Server Minimum Keep Alive Period *	[0-Unlimited] Value is time in seconds. Default = 0 seconds.

* This mechanism is used in coordination with the refreshing of NAT bindings. Specifically, in conjunction with use of Restricted Cone NAT or Port Restricted Cone NAT (as may be configured in some gateways). A device's internal address / port mappings, which the STUN protocol is allowed to make use of, can have keep alive values attributed. These minimum and maximum keep alive times define respectively, the minimum time to retain the mapping information STUN has discovered, and the maximum time to retain that information, before refreshing it through forced re-discovery.

With the above-mentioned NAT schemes it is possible the network address translation initially established may not be used after a specified elapsed time. Such internal mapping is dropped. The gateway will then assign a different address mapping. This mechanism within the STUN protocol allows for coordinated refresh on the bindings for mappings it uses. For further information, review STUN-related RFCs.

Selecting appropriate values for these two fields are influenced by a variety of environmental factors including devices types deployed, services employed and NAT configuration options enabled within the topology.

Internet Time

Sync the clock in your gateway with reliable external clocking servers available on the Internet.

After selecting **Management -> Internet Time** you may check the checkbox on the first line to enable the Network Time Protocol. You may select or input your own NTP servers.

Select the desired time zone for the gateway.

Click **Apply/Save** to commit your settings.

SMART/RG®
forward thinking

Time settings

This page allows you to change the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov

Second NTP time server: clock.via.net

Third NTP time server: None

Fourth NTP time server: None

Fifth NTP time server: None

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

Apply/Save

Access Control

Accounts

Your SmartRG Gateway can support multiple logins to its on-board user interface. Each login can be created to vary in available access privileges to pages in the CPE UI. This is particularly useful when an ISP wishes to limit access available to their subscribers, yet maintain full access by their technical support and on-site installer personnel.

NOTE: This feature requires firmware v2.5.0.7 and above.

After selecting **Management -> Access Control -> Accounts**, click **Create Account** to set up a new user. The following screen appears.

SMART/RG®
forward thinking

Create Account

Username:

Password: ☐ Show Password

Assign Privileges

☐ Device Info	☐ Wireless
☐ Summary	☐ Basic
☐ WAN	☐ Security
☐ Statistics	☐ MAC Filter
☐ Route	☐ Wireless Bridge
☐ ARP	☐ Advanced
☐ DHCP	☐ Station Info
☐ Advanced Setup	☐ Diagnostics
☐ Layer 2 Interface	☐ Diagnostics
☐ WAN Service	☐ Fault Management
☐ 4G LTE Settings	☐ Ping Host
☐ Ethernet Config	
☐ LAN	

Menu: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, Security Log, SNMP Agent, Management Server, Internet Time, Access Control, **Accounts**, Services, Passwords, Access List, Logout Timer, Update Software, Reboot, Logout

1. Enter a **Username** and **Password** for the new account.
2. Check the boxes* for each feature you wish this user to have access to
3. Click **Save Account** to commit your changes. Your new account has been created. You must log out to test.

* If you check the beginning sub category to the left, the subordinate boxes for that section will automatically be selected.

Modify or Delete an Account

NOTE: You can NOT modify or delete the default Users: Admin, Support, MFG, or User. The option to disable the **Support**, **MFG**, or **User** however is available. You must be logged into the gateway as the Admin or Support user in order to modify or delete any accounts.

SMART/RG®
forward thinking

Delete/Edit Account

Select an account :

Enable/Disable account: ☒ Enable ☐ Disable

Username:

Password: ☐ Show Password

Assign Privileges

☒ Device Info	☒ Wireless
☒ Summary	☒ Basic
☒ WAN	☒ Security
☒ Statistics	☒ MAC Filter
☒ Route	☒ Wireless Bridge
☒ ARP	☒ Advanced
☒ DHCP	☒ Station Info
☐ Advanced Setup	☒ Diagnostics
☐ Layer2 Interface	☒ Diagnostics
☐ WAN Service	☒ Fault Management
☐ 4G LTE Settings	☒ Ping Host
☐ Ethernet Config	☒ Trace Route to Host
☐ LAN	☐ Management
☐ NAT	☐ Settings
☐ Security	☐ System Log
☐ Parental Control	☐ Security Log
☐ Quality of Service	☐ SNMP Agent
☐ Routing	☐ Management Server
☐ DNS	☐ Internet Time
☐ DSL	☐ Access Control
☐ DSL Bonding	☐ Update Software
☐ UPnP	☐ Reboot
☐ DNS Proxy	☐ Support Tools
☐ Interface Grouping	☐ Port Mirroring
☐ IP Tunnel	☐ Factory reset
☐ IPSec	
☐ Certificate	
☐ Multicast	

© 2012-2015 SmartRG Inc. All Rights Reserved.

1. From the left navigation bar, select **Management -> Access Control -> Accounts** then click, **Delete/Modify Account**.
2. Click the, **Select an account** drop-down and click the account you wish to modify or delete.
3. To Modify - Check or uncheck the desired boxes. Click **Update Account** to commit your changes.
4. To Delete – Scroll to the bottom of the page and click **Delete Account**.
5. To Disable/Enable the account you've selected– Toggle the **Enable/Disable account**: buttons.

Default Passwords:

USER	PASSWORD
admin	admin
support	support
user	user
mfg	IDH7iw@ibRsPOIBa

Services

Utilize this screen to establish a Service Control List. You may control which services (FTP, HTTP, Telnet, etc.) are to be restricted on the LAN.

After selecting **Management -> Access Control -> Services** you may modify settings as desired.

Click **Apply/Save** to commit your settings.



- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Settings
- System Log
- Security Log
- SNMP Agent
- Management Server
- Access Control
- Services**
- Passwords
- Access List
- Logout Timer
- Update Software
- Reboot
- Logout

Access Control -- Services

A Service Control List ("SCL") is used to enable or disable network services on the gateway.
Note: LAN side firewall must be enabled to modify LAN SCLs.

Services	LAN
HTTP(S)	☒ Enable
☐ Use encrypted HTTP(S) -- unit will restart.	
FTP	☒ Enable
ICMP	Enable
SNMP	☒ Enable
SSH	☒ Enable
TELNET	☒ Enable
TFTP	☒ Enable

Save/Apply

The individual fields on this screen are defined as follows:

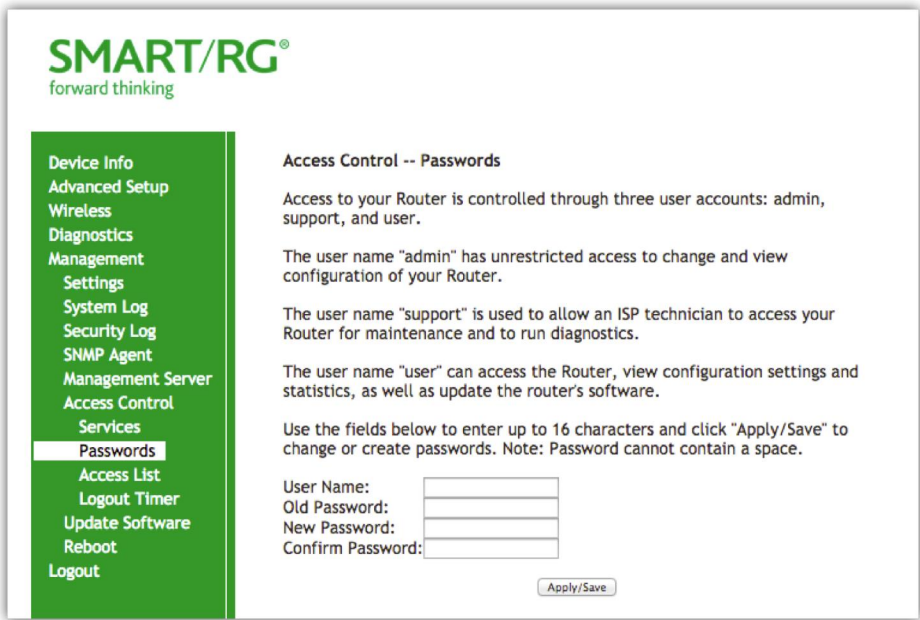
Field Name	Description
Services	[FTP, HTTP, ICMP, SNMP, SSH, TELNET, TFTP] Specifies the SCL services that can be enabled or disabled via the Access Control configuration screen.
LAN	Specifies service enabled (via checkbox) on LAN side firewall. Note: ICMP is an always-enabled service by default and has no checkbox.
WAN	Specifies service enabled on the WAN side firewall.
WAN Port Number	Specifies the port the access control applies to on the WAN side for the given service. See port information below.
Service Control List service: FTP	FTP Service access (For WAN this is with default port).
Service Control List service: HTTP	HTTP Service access (For WAN this is in association with port specified " default is port 80).
Service Control List service: ICMP	ICMP Service access (For WAN this is with default port).
Service Control List service: SNMP	SNMP Service access (For WAN this is with default port).
Service Control List service: SSH	SSH Service access (For WAN this is in association with port specified " default is port 22).
Service Control List service: TELNET	TELNET Service access (For WAN this is with default port).
Service Control List: TFTP	TFTP Service (as with default port) Access.

Passwords

Establish or alter the passwords associated with access to the Gateway. Three accounts are available to manage: Admin, Support and User.

After selecting [Management -> Passwords](#) you enter your desired settings for one login.

Click [Apply/Save](#) to commit your settings.



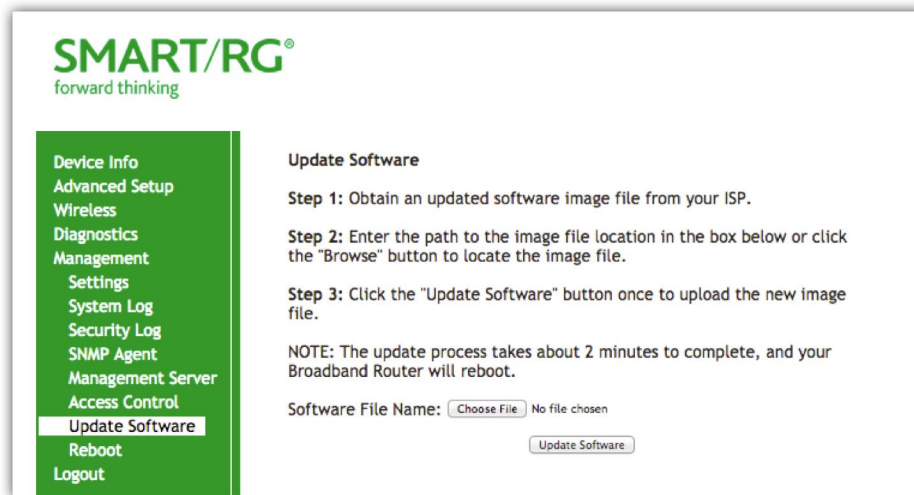
The individual fields on this screen are defined as follows:

Field Name	Description
User Name	[admin, support, user] Specifies name of account to be configured.
Old Password	Enter the current password being acted on for the entered User Name. It is termed the old password as the subsequent fields will replaces it with a new password.
New Password	The new password being chosen for the entered User Name. (Max 16 characters.)
Confirm Password	Re-enter the desired new password exactly as entered for the previous field.

Update Software

Utilize this feature to update the firmware of your SmartRG gateway. Software updates for SmartRG product are available for download by direct customers of SmartRG via the SmartRG Customer Portal.

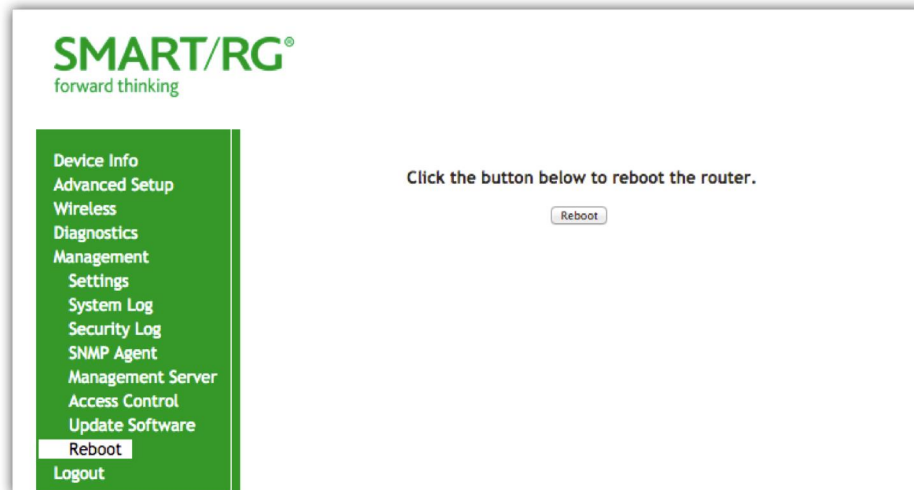
Select **Management -> Update Software** from the left navigation bar. The following screen will appear. Follow the on-screen instructions.



Reboot

Occasional troubleshooting measures may require that the router be rebooted. The reboot function is located on this screen.

Select **Management** -> **Reboot** from the left navigation bar. The following screen will appear.



Appendix A: Advanced Features Overview

This appendix outlines the advanced feature set for SmartRG brand home gateway products.

Connect-and-Surf (Automatic Broadband Connection Configuration)

The Connect-and-Surf feature automatically establishes a WAN connection for default-configured gateways obviating the need for manual or custom configurations. The active physical layer is detected (ADSL, VDSL or GigE) and layer 3 connectivity is established using PPP authentication or DHCP.

NOTE: If you prefer to configure your SmartRG's WAN interface manually, connect a laptop to any of the LAN ports and follow the instructions in the "Logging in to Your SmartRG Gateway" and "Remote Management" sections of this User Manual. Do not connect the WAN interface cable until after the configuration is completed.

Activation (Automatic ACS Connection Configuration)

SmartRG gateways are designed to discover their service provider-specific ACS management settings without the use of custom firmware. SmartRG Inc. maintains an activation server that associates a device's MAC address with its service provider's ACS settings. SmartRG gateways contact the activation server to have their ACS settings modified upon initial power up (or after being reset to factory default settings).

NOTE: Activation server support is provided for ALL SmartRG gateways at no additional cost. SmartRG Inc. enters gateway MAC addresses into the activation server prior to shipment.

TR-069 Remote Management: Automated Configuration Server Support

With a rich TR-069 heritage and a strong commitment to standards based, remote management, SmartRG gateways are designed for maximum interoperability with industry leading, TR-069-based remote management systems. SmartRG gateways provide maximum remote manageability and the highest level of visibility into the connected home yielding:

- Shorter integration times
- Lower system integration costs
- Improved customer support
- Reduced operational expenses

SMART/RG

SmartRG works closely with industry-leading, TR-069 automated configuration server (ACS) solutions providers to ensure "plug-n-play" interoperability. See following table.



Calix Compass/Consumer Connect ACS

In addition to being Calix physical layer certified (to ensure Calix access equipment compatibility), SmartRG gateways have been tested to confirm maximum interoperability with the Calix Compass/Consumer Connect ACS solution.



Affinegy ACS

SmartRG gateways have been tested to confirm maximum interoperability with the Affinegy ACS solution.



Cisco Prime Home™ ACS

SmartRG gateways have a long history of Prime Home (formerly ClearVision) ACS interoperability.

Appendix B: Feature Comparison Matrix

SmartSG residential gateways combine WAN connectivity with a firewall-protected router and industry-leading TR-069 remote management support. Most variants provide 802.11n Wi-Fi connectivity, as well. See the model-specific, SmartSG feature details below:

Model	Broadband Connection	LAN ports	LAN Device Discovery	Managed Firewall	Managed Wi-Fi	Wi-Fi Signal Monitor	IPv6	IPTV Ready
SR552n	Tri-mode: ADSL2+, VDSL2, GigE	5 GE	✓	✓	802.11n	✓	✓	✓
SR550n	Tri-mode: ADSL2+, VDSL2, GigE	3 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR510n	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR505n	Tri-mode: ADSL2+, VDSL2, GigE	3 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR500n	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR400ac	Gigabit Ethernet	5 GE	✓	✓	Dual-band concurrent 802.11ac	✓	✓	✓
SR360n	ADSL2+, Ethernet	4 FE	✓	✓	802.11n	✓	✓	✓
SR350N	ADSL2+	4 FE	✓	✓	802.11n	✓	✓	✓
SR350NE	Ethernet	4 FE	✓	✓	802.11n	✓	✓	✓
SR100	ADSL2+	4 FE	✓	✓				
SR10	ADSL2+	1 FE	✓	✓				

Contact SmartSG Support for detailed descriptions and management of the features listed above.

Revision History

Rev	Date	LAN ports
3.0	6/26/2014	Complete re-write New layout Authored complete field-by-field descriptions for each screen Complete compendium of screen-shots for each feature Migrated use case content to on-line knowledge base. (See the SmartRG Customer Portal.)
3.2	10/20/2014	Visual overhaul. New colors, logo and layout. Added missing sections for Ethernet Config and LAN. Expanded chapters for Management Server and STUN.
3.3	1/28/2015	Cosmetic enhancements. Replaced screen shots with new UI color scheme and logos. Expanded coverage of Advanced Setup -> WAN Service. General edit
3.4	6/20/2015	Updated behavior description for the reset button for FW v2.5.0.7 Clarified WLAN button operation with press and hold durations Expanded the field definitions for xDSL Statistics screen Expanded the definition for the MTU Size field added to the PPP Usernam and Password screen Added section for Access Control (new feature in FW v2.5.0.7). Corrected the table content for the fields seen on the NAT screen found in the IPoE WAN interface workflow Added section for LAN -> IPv6 Autoconfig (inadvertently omitted from previous versions). Miscellaneous formatting and content corrections Implemented image compression to reduce .pdf file size